# La protection des données dans les contrats de cloud computing

Sarah Sadik

# THÈSE

Pour obtenir le grade de

Docteur

**Délivrée par**

**UNIVERSITE DE PERPIGNAN VIA DOMITIA**

Préparée au sein de l'école doctorale 544 INTER-MÉD : Espaces, Temps, Cultures
Et de l'unité de recherche EA 4216 Centre de Droit Économique et du développement Yves Serra

**Spécialité : Droit privé**

**Présentée par Sarah SADIK**

# La protection des données dans les contrats de cloud computing

Soutenue à Perpignan le 23 janvier 2023 à 10h

devant le jury composé de

| | |
|---|---|
| M. Yves PICOD, Professeur de droit privé, Université de Perpignan Via Domitia | Directeur de thèse |
| M. Sylvain CHATRY, Maître de conférences, Université de Perpignan Via Domitia | Co-directeur de thèse |
| Mme Alexandra MENDOZA-CAMINADE, Professeur de droit privé, Université de Toulouse 1 Capitole | Présidente |
| Mme Jessica EYNARD, Maître de conférences, Université de Toulouse 1 Capitole | Rapporteuse |
| Mme Agnès ROBIN, Maître de conférences, Université de Montpellier | Rapporteuse |

Avertissement : La Faculté n'entend donner aucune approbation ni improbation aux opinions émises dans cette thèse ; ces opinions doivent être considérées comme propres à leur auteur.

A ma famille et mes proches pour leur soutien.

# REMERCIEMENTS

Je tiens, tout particulièrement, à remercier le Professeur Yves PICOD d'avoir accepté d'être mon directeur de thèse, de sa confiance et de son soutien tout au long de ma thèse. Je remercie, également, mon co-directeur de thèse, Monsieur Sylvain CHATRY, de son implication bénéfique dans l'élaboration de ma thèse, de ses précieux conseils et de sa disponibilité. Je suis honorée et reconnaissante d'avoir réalisé ma thèse sous vos directions bienveillantes.

Je remercie la Professeure Alexandra MENDOZA-CAMINADE, Madame Jessica EYNARD, Madame Agnès ROBIN qui m'ont fait l'honneur de bien vouloir être membres de mon jury et du temps que vous avez consacré à ma thèse.

J'ai une pensée particulière à l'endroit de Madame Suzanne GILARDOT et Madame Hélène GUISSET qui m'ont accordé du temps et un appui administratif depuis mon inscription en doctorat.

Je remercie, également, l'École doctorale de m'avoir permis de réaliser ma thèse dans un cadre propice à la stimulation intellectuelle et à l'échange entre les étudiants issus de différentes disciplines.

La réalisation de ma thèse a été pour moi une expérience riche tant au niveau intellectuel que personnel. Ma reconnaissance et ma gratitude reviennent à tous ceux et celles qui se sont présentés sur mon chemin et ont eu un impact positif sur l'aboutissement de ma thèse.

# SOMMAIRE

# PRINCIPALES ABRÉVIATIONS

ADPIC : Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce

Aff. : Affaire

AJ : Actualité jurisprudentielle (du Recueil Dalloz)

al. : Alinéa

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

art. : Article

AUP : Acceptable Use Policy (traduction : l'acceptation de la politique d'utilisation)

BCR : Binding corporate rules

Bull. civ. : Bulletin des arrêts de la Cour de cassation : chambres civiles

Bull. com. : Bulletin des arrêts de la Cour de cassation : chambre commerciale

Bull. crim : Bulletin des arrêts de la Cour de cassation : chambre criminelle

C./ : Contre

C. civ. : code civil

C . com. : code de commerce

C. consom. : code de la consommation

CA : Cour d'appel

Cass. Ass. plén. : Assemblée plénière de la Cour de cassation

Cass. civ. : Chambre civile de la Cour de cassation

Cass. com. : Chambre commerciale de la Cour de cassation

Cass. crim. : Chambre criminelle de la Cour de cassation

Cass. soc. : Chambre sociale de la Cour de cassation

CCP : Code de la commande publique

CRPA : Code des relations entre le public et l'administration

CE : Conseil d'État

CEPD : Comité européen de la protection des données

CEPD : Contrôleur européen de la protection des données

CES : Conseil économique et social

CESE : Comité économique et social européen

Ch. : Chambre

Chron. : Chronique

Cloud Act : Clarifying Lawful Overseas Use of Data Act

CNIL : Commission nationale de l'informatique et des libertés

CNUCED : Conférence des Nations unies sur le commerce et le développement

Coll. : collection

Comm. : commentaire

Comm. com. électr. : Communication commerce électronique

Concl. : Conclusions

Contra : en sens contraire

Conv. : Convention

CPI : Code de la propriété intellectuelle

C-SIG : Cloud select industry group

CJCE : Cour de justice des Communautés européennes

CJUE : Cour de justice de l'Union européenne

Dir. : directive

DES : Data Encryption Standard

DDHC : Déclaration des droits de l'homme et du citoyen

doctr. : doctrine

éd. : édition

EEE : Espace économique européen

fasc. : fascicule

Gaz. pal. : gazette du palais

Gaz. trib. : gazette des tribunaux

Gr. ch. : Grande chambre

G29 : Groupe de l'article 29

IaaS : Infrastructure as a Service

*ibid*. : ibidem (au même endroit)

idem : dans le même sens

*in* : dans

*infra* n° : ci-dessous au paragraphe n°

INPI : Institut national de la propriété industrielle

J.-Cl. : JurisClasseur

JCP E : La Semaine juridique, édition entreprise et affaires

JCP G : La Semaine juridique, édition générale

JO : Journal officiel

JORF : Journal officiel de la République française

JOEU : Journal officiel de l'Union européenne

Juris : Jurisprudence

KPI : Key Performance Indicators

n° : numéro

NOYB : (association) None Of Your Business

NTIC : nouvelles technologies de l'information et de la communication

Obs. : observations

OMPI : Organisation mondiale de la propriété intellectuelle

*Op. cit.* : opus citatum (ouvrage précité)

Ord. : ordonnance

p. : page

PaaS : Platform as a Service

pan. : panorama

PME Petites et moyennes entreprises

Propr. ind. : Propriété industrielle

Propr. intell. : Propriétés intellectuelles

Pt. : point

RDC : Revue des contrats (Lextenso)

RDNP : Règlement des données à caractère non personnel

Rec. : Recueil de la Cour de justice et du Tribunal de l'Union européenne

RFDA : Revue Française de Droit Administratif

règl. : Règlement

Rép. civ. : Répertoire Dalloz de droit civil

Rép. com. : Répertoire Dalloz de droit commercial

RG : Répertoire général

RGPD : Règlement général sur la protection des données

RLDA : Revue Lamy droit des affaires

RLDI : Revue Lamy droit de l'immatériel

s. : suivant(e)s

SaaS : Software as a Service

sect. : section

SSL : Secure Sockets Layer ; en français « couches de sockets sécurisés »

SLA : Service Level Agreement (traduction : convention de services)

somm. : sommaire(s)

SOW : Statement of work (traduction : cahier des charges)

SQL : Structured Query Language : en français, langages de requêtes structurées

spéc. : spécialement

ss. : sous

sous la dir. de : sous la direction de

suppl. : supplément

*supra* n° : ci-dessus au paragraphe n°

t. : Tome

T. corr. : Tribunal correctionnel

TFUE : Traité sur le fonctionnement de l'Union européenne

TGI : Tribunal de grande instance

TLS : Transport Layer Securité ; en français « sécurité de la couche de transport »

TPE : Très petites entreprises

TCP/IP : Transfert Control Protocol/Internet

Trib. UE : Tribunal de l'Union européenne

TUE : Traité sur l'Union européenne

UE : Union européenne

v. : Voir

vol. : volume

v° : verbo (mot)

# - INTRODUCTION GÉNÉRALE

« Il importe de relever qu'une matière juridique peut subir des modifications en profondeur et qu'on discute justement sur la profondeur atteinte. Si la nouveauté n'affecte que des régions superficielles, elle sera assimilée, au prix peut-être d'une transformation d'elle-même comme de la région affectée. Si elle concerne au contraire la zone profonde, elle sera rejetée ou disloquera le système ».[1]

[1]Batiffol H., Aspects philosophiques du droit international privé, Dalloz, Paris, 2002 (1956), pp.50-51.

***1.*** Alors que les nouvelles technologies de l'information et de la communication (NTIC) ont bouleversé nos rapports au monde et aux autres dans sa globalité, le droit a su résister, s'affirmer et innover en établissant de nouveaux concepts et un cadre juridique qui puissent être à la fois contraignants et soucieux des droits et libertés individuels. Ce cadre juridique est particulier en fonction de l'État où l'application du droit est demandée bien qu'il soit caractérisé, aujourd'hui, par un renforcement d'un cadre juridique transnational. Par ailleurs, il est bien évidemment question aujourd'hui d'une quête d'adaptation aux NTIC voulue par les États eux-mêmes en permettant la création d'un cadre juridique développé à l'échelle nationale et européenne[2], en particulier en matière de cloud computing[3]. Cette nouvelle organisation de l'économie numérique s'inscrit dans un contexte de mondialisation, d'autant plus vrai lorsqu'il s'agit du cloud computing puisque cette technologie fait appel à un réseau internet qui ignore les frontières des États.

***2.*** La croissance fulgurante de la technologie du cloud computing et le recours massif aux contrats de cloud computing[4] ont suscité l'intérêt de réaliser une thèse dédiée à cette figure contractuelle sous l'angle de la protection des données. La donnée est considérée comme étant « la matière première des échanges entre les hommes »[5]. Il est constaté que « la protection et la sécurité des données personnelles et numériques, avec notamment le récent et rapide développement du cloud computing et du big data, suscitent une attention particulière des entreprises et des professionnels du droit tant au niveau national qu'international »[6].

***3.*** Tel qu'affirmé par Monsieur Sauvé, « sous l'appellation poétique d'« informatique en nuage », se cachent, certes une promesse de progrès, mais aussi, tâchons de ne pas l'oublier, la violence qui peut procéder de l'absence – par déréglementation – et de l'ignorance du droit. Il en résulte pour les personnes des risques qui, pour reprendre la terminologie du sociologue Ulrich Beck, sont irréversibles et pourtant majoritairement invisibles, des risques « réels et irréels à la

---

[2] Castets-Renard C., Ndior V., Rass-Masson L., Enjeux internationaux des activités numériques, Entre logique territoriale des États et puissance des acteurs privés, édition Larcier, collection Création Information Communication, septembre 2020 : « Les États n'ont pas renoncé à leur souveraineté légale ni à encadrer le comportement d'acteurs qui pensaient pourtant pouvoir s'affranchir de la règle de droit. Ils tendent à illustrer aussi que cet encadrement prend souvent des traits originaux en comparaison des mécanismes juridiques classiques. Ils invitent ainsi à s'interroger sur le sens et la forme, éventuellement renouvelés, de la règle de droit, tant du moins qu'est affirmée la volonté de réguler ou de réglementer l'activité numérique à l'échelle internationale par le droit ».

[3] Illustration avec la Proposition de Règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (Acte sur la gouvernance des données- « AGD »), 2020/0340 (COD), publiée le 25 novembre 2020 dont l'objectif est de favoriser le partage des données entre les secteurs et les États membres. Il s'agit d'un nouveau mode de nouveau mode de gouvernance des données pour renforcer la confiance dans le partage des données, les mécanismes visant à accroître la disponibilité des données et pour surmonter les obstacles techniques à la réutilisation des données.V. également, Quiquerez A., Actualité du droit des technologies nouvelles (février - juin 2020), revue Lamy Droit Civil, 1er septembre 2020, numéro 184, page(s) 25-36.

[4] Briffaut J.,P. et Stephan F., Cloud computing, évolution technologique, révolution des usages, Lavoisier, 2013

[5] Bourgeois M., Droit de la donnée, principes théoriques et approche pratique, LexisNexis, 2017.

[6] Bitan H., Droit et expertise du numérique, Créations immatérielles, Données personnelles, E.réputation, Droit à l'oubli, Neutralité, Responsabilité civile et pénale, édition Lamy, collection Axe droit, Wolters Kluwer, juin 2015.

fois »[7] »[8]. Cette déclaration souligne à quel point, il est complexe d'appréhender juridiquement cet objet qu'est le cloud computing.

***4.*** Dans le cadre de l'utilisation d'un service de cloud computing, les données sont confiées à un tiers auquel il faut faire confiance. On perçoit immédiatement les risques pour des utilisateurs (personne physique et personne morale) d'un service de cloud computing de laisser leurs données transiter hors de leurs propres installations[9]. La formalisation d'un contrat de cloud computing suscite des interrogations juridiques et en particulier la question de l'effectivité du droit dans un environnement globalisé[10]. Au niveau de la pratique, le cloud computing a suscité des questionnements, tels que ceux abordés dans le cadre d'un colloque « quels sont les enjeux suscités par le cloud computing ? Appelle-t-il une définition unitaire ou impose-t-il de retenir une approche plurale pour identifier les différents acteurs et services offerts ? Doit-on penser de nouveaux instruments de régulation ? Comment assurer la protection des données à caractère personnel alors que l'on s'interroge sur leur localisation ? Quel modèle contractuel envisager afin de garantir l'intégrité, la sécurité et la confidentialité des données ainsi que leur réversibilité ? »[11]. Encore aujourd'hui, le cloud computing conserve, pour une grande partie de la population, une part de mystère. Tel qu'affirmé par Monsieur Sauvé, « le cloud est un phénomène qui échappe encore à notre maîtrise et même à notre compréhension. Alors même qu'il est susceptible d'affecter chaque citoyen, chaque entreprise et chaque personne publique, alors même qu'il renouvelle les modèles économiques et interroge nos catégories juridiques, il conserve une part de mystère qui n'en est que plus étonnante »[12]. Également, des inquiétudes ont été soulevées par des auteurs quant à l'essor des technologies sur la vie privée des individus, considérant que « le constat de départ était celui d'une dangerosité accrue des moyens informatiques pour les libertés du citoyen »[13].

---

[7] Beck U., La société du risque. Sur la voie d'une autre modernité, Paris, Champs Flammarion, 2003, p. 40.

[8] Sauvé J-M, Le cloud computing, colloque de la Société de législation comparée au Conseil d'État, 11 octobre 2013 : https://www.conseil-etat.fr/publications-colloques/discours-et-interventions/le-cloud-computing#40.

[9] Winkler V.J.R., La sécurité dans le Cloud. Techniques pour une informatique en nuage sécurisée, Pearson, Paris, 12 octobre, 2011.

[10] Papin E., Que se cache-t-il derrière la nébulosité des contrats de Cloud Computing?, 16 déc. 2014, www.cio-online.com.

[11] Fauvarque-Cosson B., et Zolynski C., Le Cloud Computing, L'informatique en nuage, Société de législation comparée, collection Colloques, juin 2014.

[12] Sauvé J-M, Le cloud computing, colloque de la Société de législation comparée au Conseil d'État, 11 octobre 2013 : https://www.conseil-etat.fr/publications-colloques/discours-et-interventions/le-cloud-computing#40.

[13] Benabou V.-L., L'extension du domaine de la donnée, revue Légipresse, 1er avril 2018, numéro 359, page(s) 197-207 : « La technique ayant facilité la numérisation des informations, l'ensemble des données que l'on peut rattacher à un individu est désormais traduit dans une écriture unique, susceptible d'un traitement rapide et peu coûteux, d'une duplication à l'infini sans dégradation de qualité. Le développement des réseaux permet la multiplication des échanges économiques ou personnels d'informations, là encore pour un coût très faible. L'économie s'étant orientée vers les échanges intangibles, les données sont devenues des « actifs » dont la valeur patrimoniale suscite tous les appétits. Ainsi la corrélation des facteurs techniques, économiques et sociétaux a mis les données au cœur des échanges humains, à une échelle inédite. On parle de « Big Data*» (*Voir Babinet G., Big Data, Penser le monde et l'homme autrement, Le Passeur, 2015 qui définit le concept autour de l'existence d'une masse de données traitées par une architecture distribuée tout en rappelant l'approche des trois V : Volume, Vélocité, Variété, ultérieurement complétée par les deux V de Valeur et de Véracité.) Dès lors, ce qui pose un problème est l'extension infinie du champ des menaces qui pèsent sur l'individu

***5.*** Cette thèse a pour objet d'étudier la protection des données des personnes physiques[14] et des personnes morales de droit privé dans les contrats de cloud computing. Les données des personnes morales appartiennent à la catégorie des données à caractère non personnel et sont regroupées dans ce que la doctrine nomme « le patrimoine informationnel »[15]. En revanche, il est fait le choix d'exclure du champ de l'étude de la protection des données des personnes morales de droit public. Pour justifier cette exclusion, il est estimé que les enjeux de protection des données dans les contrats de cloud computing concernent principalement les personnes physiques et les personnes morales de droit privé parties à un contrat de cloud computing. En effet, lorsque les personnes morales de droit public utilisent la technologie du cloud, elles peuvent, tout d'abord, bénéficier de règles spécifiques pour la protection de leurs données sensibles en recourant au cloud souverain par exemple et quant aux autres données des administrations elles sont majoritairement soumises aux principes de l'*open data* et de la libre réutilisation desdites données [16]. S'agissant des données sensibles, les personnes morales de droit public peuvent exiger que celles-ci (telles les données afférentes à la sécurité nationale) soient stockées dans des centres de données (datacenters[17]) situés en France, et ce afin de préserver la souveraineté nationale [18]. Tel qu'affirmé par Monsieur Watin-Augouard, « la gouvernance d'Internet devient un enjeu de puissance et de souveraineté »[19]. L'utilisation du cloud souverain[20] par les personnes morales permet, dans ce sens, de se prémunir contre la délocalisation de ses données hors des frontières de l'État et ainsi de réduire les risques d'atteinte à celles-ci. À cette fin, une circulaire administrative a été adressée aux administrations

---

du fait du traitement de « ses » données ». V. Beky A., peu de services Cloud conformes au futur droit européen sur les données, 13 août 2014, disponible sur https://www.silicon.fr/fournisseurs-cloud-reglement-data-protection-europe-96121.html. V. Bourcier D. et Primavera De Filippi P., Open data & big data, nouveaux défis pour la vie privée, mare &martin, 2016.

[14] Les données à caractère personnel des personnes physiques correspondent à toutes les informations susceptibles d'identifier une personne physique.

[15] Saint-Aubin Th., les nouveaux enjeux juridiques des données (big data, web sémantique et linked data) Les droits de l'opérateur de données sur son patrimoine numérique informationnel, Revue Lamy Droit de l'Immatériel, N° 102, 1er mars 2014.

[16] Ord. n° 2005-650, 6 juin 2005 , relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques : AJDA 2006, p. 1377, comm. B. Delaunay.

[17] Définition : « En anglais, « data center » signifie « centre de traitement de données ». Il s'agit d'un lieu sur lequel sont rassemblé des équipements informatiques lié au système d'information d'une entreprise. Ce centre de traitement peut être interne et/ou externe et exploité ou non avec le soutien de prestataires » : https://www.silicon.fr/actualites/cloud/datacenter.

[18] Le Tourneau Ph., Contrats du numérique, informatiques et électroniques, 12e édition, 2022-2023 : Au niveau de la doctrine, le caractère nébuleux du cloud dans les contrats de cloud computing (dispersion des serveurs) a suscité des interrogations et des inquiétudes sur la protection des données.

[19] Watin-Augouard M., La cybersécurité, enjeu de la souveraineté à l'ère numérique, Dalloz IP/IT 2021 p.130.

[20] Définition de cloud souverain : « le cloud est dit « souverain » lorsque les données doivent être entièrement stockées et traitées sur le territoire d'un État » : Wagener N., Cloud souverain et archives publiques, JAC 2017, n° 43, p. 38. V. également, Le Quellenec E., L'émergence d'un cloud souverain européen, revue Lamy droit de l'immatériel ex Lamy droit de l'informatique, 1er août 2020, numéro 173, page(s) 37-39.

décentralisées afin de demander de recourir à un « cloud souverain »[21]. Alors, il a été considéré qu'en ne délocalisant pas ces données hors de France cela permettrait, dans une certaine mesure, de réduire les risques quant à la protection des données et les incertitudes quant à la détermination du droit applicable. Comme le souligne Monsieur Watin-Augouard, « c'est sans doute parce qu'ils possèdent une certaine souveraineté numérique que les États peuvent s'inscrire dans une démarche conventionnelle qui les oblige »[22]. Aujourd'hui, le recours au cloud souverain par les personnes morales de droit public est remis en question par le droit de l'Union européenne lorsqu'il s'agit de données à caractère non personnel. Dès lors que les données concernées sont des données à caractère non personnel, le Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018[23] exige des États le libre flux de celles-ci au sein de l'Union européenne. Dorénavant, la France et les autres États membres ont dû se conformer avant le 31 mai 2021 à l'esprit et à la lettre de ce nouveau texte. En conséquence, il n'est plus permis pour un État de conserver ou d'adopter des dispositions faisant obstacle à la libre circulation des données à caractère non personnel au sein de l'Union européenne sauf à pouvoir justifier d'un intérêt de sécurité publique[24]. En définitive, les personnes morales de droit privé ou de droit public peuvent stocker les données à caractère non personnel auprès d'un prestataire de services dont les datacenters (centre de traitement des données) se situent hors des frontières de l'État. Comme le souligne Monsieur Dèbes, cela « n'est pas sans implications pour le projet politique, d'ailleurs assez mal engagé, de création d'un « cloud souverain »[25]. Dans l'exposé des motifs de ce texte, il est rappelé qu'« il est de la plus haute importance » que les personnes morales de droit public « montrent l'exemple en utilisant les services de traitement des données et qu'ils s'abstiennent [dans ce cadre] de prendre des mesures restrictives en matière de localisation des données ». Ce principe de libre circulation des données se heurte à la jurisprudence constante de la Cour de justice de l'Union

[21] Note d'information du 5 avril 2016 relative à l'informatique en nuage (*Cloud computing*), Réf. NOR MCCC1614354C.

[22] Watin-Augouard M., la cybersécurité, enjeu de la souveraineté à l'ère numérique, Dalloz IP/IT 2021 p.130.

[23] Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne » publié au Journal officiel le 28 novembre 2018 et entré en vigueur le 27 mai 2019.

[24] Le concept de « sécurité publique » englobe à « la fois la sécurité intérieure et extérieure d'un État membre, mais aussi les questions de sûreté publique, afin, en particulier, de faciliter la détection des infractions pénales, les enquêtes et les poursuites en la matière. Il présuppose l'existence d'une menace réelle et suffisamment grave portant atteinte à l'un des intérêts fondamentaux de la société, telle qu'une menace pour le fonctionnement des institutions et des services publics essentiels et pour la survie de la population, ainsi que le risque d'une perturbation grave des relations extérieures ou de la coexistence pacifique des nations, ou un risque pour les intérêts militaires ». Il est ajouté que le principe de proportionnalité, les exigences de localisation des données qui sont justifiées par des motifs de sécurité publique devraient être adaptées à la réalisation de l'objectif poursuivi et ne devraient pas aller au-delà de ce qui est nécessaire pour atteindre cet objectif ».

[25] Dèbes F., Une page se tourne pour le cloud souverain français, Les Échos, 1er août 2019.

européenne, consacrée dans les textes en droit interne[26], selon laquelle « le droit de l'Union européenne et plus particulièrement le droit de la commande publique n'oblige pas les personnes qui s'y trouvent soumises à recourir au contrat pour se procurer les prestations répondant à leur besoin plutôt que de les satisfaire par leurs propres moyens[27]. Malgré la consécration de ce principe de libre circulation des données au sein de l'Union européenne, le règlement autorise des entraves à la libre circulation des données dès lors qu'elles sont justifiées par des motifs de sécurité publique. Les administrations conservent, alors, la possibilité de conserver certaines données dans un cloud souverain dès lors qu'elles justifient d'un intérêt de sécurité publique.

***6.*** Outre la possibilité pour les personnes morales de droit public de bénéficier des règles spécifiques de protection de leurs données sensibles, telles que la possibilité d'exiger le stockage de leurs données dans un cloud souverain ; il apparaît que les autres données (celles ne revêtant pas un caractère sensible pour la sécurité nationale en particulier) sont intégrées dans le mouvement de l'ouverture des données (« l'open data ») promu dans les textes au niveau européen et national. À ce titre, il apparaît que le cadre juridique au niveau national et européen encourage le partage des données détenues par les personnes morales de droit public afin de servir le développement de l'innovation et de l'économie. Tel qu'affirmé par certains auteurs « très tôt, le législateur français a pris conscience de l'importance et de la valeur des données récoltées, traitées, ou encore produites par les acteurs du secteur public, notamment par l'édition de notes, de documents ou de rapports, et il a, donc, adopté un cadre permettant leur réutilisation par le secteur privé tout en les protégeant. Avec l'expansion des applications numériques dans l'espace public, il est apparu que les données numériques de l'administration sont, de la même manière que l'étaient autrefois les documents papier, des données d'importance et d'une grande valeur pour l'économie. Quant à l'administration, elle peut elle aussi être consommatrice d'innovation et ainsi participer à la transformation numérique de la cité » [28]. C'est, ainsi, pour favoriser cet *open data* qu'un cadre juridique a été établi. Concernant le régime des données publiques, la directive européenne du 17 novembre 2003 concernant la réutilisation des informations du secteur public[29] refondue dans la directive européenne du 20 juin 2019

[26] CCP, art. L1 : « Les acheteurs et les autorités concédantes choisissent librement, pour répondre à leurs besoins, d'utiliser leurs propres moyens ou d'avoir recours à un contrat de la commande publique".

[27] CJUE 11 janv. 2005, aff. C-26/03 , Stadt Halle et RPL Recynclingpark Lochau GmbH, AJDA 2005. 898, dans É. Muller, La libre circulation des données et la directive concernant la réutilisation des données du secteur public, Dalloz IP/IT 2020 p.424.

[28] Witz G. et Mariez J.-S., Les données publiques au cœur de l'IA et au service de la ville intelligente, Revue Lamy droit des affaires, N° 151, 1er septembre 2019.

[29] Dir. UE et PE Cons. n° 2003/98/CE, 17 nov. 2003, concernant la réutilisation des informations du secteur public.

concernant les données ouvertes et la réutilisation des informations du secteur public[30], affirme expressément que « les informations du secteur public constituent une source extraordinaire de données qui peuvent contribuer à améliorer le marché intérieur ». Dans cet élan d'ouverture des données détenues par les personnes morales de droit au public au service de l'amélioration du marché intérieur, il a été adopté en France des lois pour promouvoir l'ouverture des données publiques et l'utilisation de celles-ci par le public. Le droit à la réutilisation des informations publiques est codifié aux articles L. 300-1 et suivants du CRPA (Code des relations entre le public et l'administration). La loi du 28 décembre 2015 [31] et la loi « Lemaire » du 7 octobre 2016 pour une République numérique [32] ont été adoptées afin de mettre le droit français en conformité avec la directive européenne[33]. Ces réformes ont eu pour objet de favoriser l'*open data* (l'ouverture des données) et le droit à la réutilisation des informations publiques. Les données concernées sont « principalement des données publiques, mais aussi de certaines « données d'intérêt général »[34]. La doctrine a estimé que « c'est un très important gisement de données publiques que vont devoir ouvrir les collectivités, l'*open data* et la réutilisation des données publiques offrant « des promesses prestigieuses[35] tant pour renforcer la démocratie par une transparence accrue que pour permettre l'éclosion de nouvelles activités et services innovants »[36]. La loi du 7 octobre 2016 pour une république numérique a élargi la liste des documents administratifs communicables aux « codes sources[37] » et que par cette énumération, il est rappelé que ces documents, quelle que soit leur forme est communicable à toute personne qui en fait la demande [38]. Ainsi, figure à l'article L. 312-1-1 du CRPA une obligation de diffusion des données. En particulier, les administrations doivent « publier en ligne, lorsqu'ils sont disponibles sous forme

[30] Dir. UE PE Cons. n° 2019/1024, 20 juin 2019, concernant les données ouvertes et la réutilisation des informations du secteur public (refonte).

[31] L. n° 2015-1779, 28 déc. 2015 , relative à la gratuité et aux modalités de la réutilisation des informations du secteur public : JO 29 déc. 2015, texte n° 4.

[32] Loi n° 2016-1321, 7 oct. 2016 pour une république numérique, Titre Ier : JO 8 oct. 2016, texte n° 1.

[33] Dir. 2013/37/UE, 26 juin 2013, modifiant la directive 2003/98/CE du 17 novembre 2003 concernant la réutilisation des informations du secteur public.

[34] Delaunay B., *l'open data dans les collectivités territoriales*, La Semaine Juridique Administrations et Collectivités territoriales n° 42, 22 octobre 2018, 2286.

[35] Open data et réutilisation des données publiques : des promesses prestigieuses : Gaz. cnes, dossier électronique : www.lagazettedescommunes.com/dossiers/reutilisation-des-donnees-publiques-des-promesses-vertigineuses/.

[36] Delaunay B., l'open data dans les collectivités territoriales, La Semaine Juridique Administrations et Collectivités territoriales n° 42, 22 octobre 2018, 2286.

[37] Définition des documents communicables aux « codes sources » : Article L. 300-2 du code des relations entre le public et l'administration « « Constituent de tels documents notamment les dossiers, rapports, études, comptes rendus, procès-verbaux, statistiques, instructions, circulaires, notes et réponses ministérielles, correspondances, avis, prévisions, codes sources et décisions »

[38] L'accès au public des documents administratifs : Article L. 300-4 du code des relations entre le public et l'administration.

électronique, les documents qu'elles communiquent (à la suite d'une demande), les documents figurant dans les répertoires des principaux documents administratifs que les administrations doivent tenir à la disposition du public [39], les bases de données produites ou reçues et les données dont la publication présente « un intérêt économique, social, sanitaire ou environnemental »[40]. La loi pour une République numérique a également « prévu la création d'un service public de l'État de mise à disposition des « données de référence », auquel sont associées les collectivités territoriales (CRPA, art. L. 321-4). Ce sont des données qui constituent une référence commune pour nommer ou identifier des produits, services, territoires ou personnes, sont réutilisées fréquemment par d'autres personnes et doivent être mises à disposition avec un niveau élevé de qualité (..) Cette large diffusion est destinée à favoriser, outre la transparence administrative, la réutilisation des informations publiques »[41]. Ensuite, le principe de la libre réutilisation des informations publiques figurant dans des documents communiqués ou publiés par les administrations est posé à l'article L. 321-1 du CRPA. Il est spécifié que ces informations peuvent faire l'objet d'une réutilisation à des fins commerciales, en l'état ou après traitement, par des opérateurs privés, notamment pour offrir de nouveaux produits ou services numériques. Ces informations publiques sont définies comme « Les informations publiques au sens de ce titre, sont des informations figurant dans des documents élaborés ou détenus par les administrations, accessibles en vertu de la législation et sur lesquels des tiers ne détiennent pas des droits de propriété intellectuelle (CRPA, art. L. 321-2) »[42]. La réutilisation de ces informations publiques est, en principe, gratuite en vertu de l'article L. 324-1 du CRPA. Ainsi, la loi du 7 octobre 2016 pour une république numérique consacre la généralisation par l'administration de la diffusion de certaines de ces données au public[43]. À titre illustratif d'accès aux données au public, la loi de programmation 2018-2022 et de réforme pour la justice[44] a intégré des dispositions pour permettre à tous l'accès aux décisions de justice au sein du code de l'organisation judiciaire[45] comme au sein du code de justice administrative[46]. À ce jour, le champ de l'*open data* est légalement large puisqu'il s'étend à l'ensemble des services publics que les données publiques soient produites par des opérateurs

[39] CRPA, art. L. 322-6.

[40] Delaunay B., l'open data dans les collectivités territoriales, La Semaine Juridique Administrations et Collectivités territoriales n° 42, 22 octobre 2018, 2286.

[41] Ibid.

[42] Ibid.

[43] Article L. 300-4 et L. 311-1 du code des relations entre le public et l'administration.

[44] Loi n° 2019-222, 23 mars 2019, de programmation 2018-2022 et de réforme pour la justice.

[45] C. org. jud. art. L. 111-13.

[46] C. just. adm., art. L. 10.

publics que par des opérateurs privés chargés de missions de service public[47]. À ce titre, il est rappelé à l'article L. 3131-2 du code de la commande publique[48] que « lorsqu'un service public est concédé, le concessionnaire doit fournir, au concédant, sous format électronique et dans un standard « ouvert librement réutilisable et exploitable par un système de traitement automatisé » les données ainsi que les bases de données qu'il collecte ou produit à l'occasion de l'exploitation du service public. Ainsi, nombre d'informations traitées par des opérateurs privés chargés de mission de service public peuvent elles aussi devenir des informations publiques parce que, par différents biais, elles remontent à l'administration. En définitive, toutes les données publiques sont soumises au principe de l'*open data* et de libre réutilisation de ces données par le public. En revanche, face à la généralisation de l'*open data* des documents administratifs, notamment en matière judiciaire, le législateur a mis en place, « des garde-fous dans le droit à la réutilisation de ce type d'informations publiques »[49]. Ces garde-fous consistent, ainsi, à titre d'exemple, en « l'occultation de tout élément permettant d'identifier les parties, les tiers, les magistrats et les membres du greffe dont la divulgation serait de nature à porter atteinte à la sécurité ou au respect de la vie privée de ces personnes ou de leur entourage, ou encore l'interdiction de réutilisation des données d'identité des magistrats et des membres du greffe ayant pour objet ou pour effet d'évaluer, d'analyser, de comparer ou de prédire leurs pratiques professionnelles réelles ou supposées »[50]. Ainsi à ce principe de libre réutilisation des données, la loi fixe des limites à la communication et à la diffusion des données au public [51], en particulier « lorsque les documents et données comportent des mentions couvertes par les secrets protégés en matière d'accès aux documents administratifs (CRPA, art. L. 311-5 et L. 311-6), ils ne peuvent être rendus publics qu'après avoir fait l'objet d'un traitement permettant d'occulter ces mentions. Et, sauf dispositions législatives contraires ou si les personnes intéressées ont donné leur accord, lorsque ces documents et données comportent des données à caractère personnel, ils ne peuvent être rendus publics qu'après avoir fait l'objet d'un traitement permettant de rendre impossible l'identification de ces personnes »[52].

[47] Witz G. et Mariez J.-S., Les données publiques au cœur de l'IA et au service de la ville intelligente, Revue Lamy droit des affaires, N° 151, 1er septembre 2019. V. également, Robin A., L'ouverture des données publiques scientifiques : de l'examen de la règle « open as possible, closed as necessary », Communication Commerce électronique n° 9, Septembre 2020, étude 15.

[48] Article L. 3131-2 du code de la commande publique reprenant une disposition que la loi pour une république numérique avait introduite à l'article 17 de l'ordonnance no 2016-65 du 29 janvier 2016 relative aux concessions.

[49] Witz G. et Mariez J.-S., Les données publiques au cœur de l'IA et au service de la ville intelligente, Revue Lamy droit des affaires, N° 151, 1er septembre 2019.

[50] Ibid.

[51] CRPA, art. L. 312-1-2.

[52] Delaunay B., l'open data dans les collectivités territoriales, La Semaine Juridique Administrations et Collectivités territoriales n° 42, 22 octobre 2018, 2286. Pour une illustration avec les données scientifiques, v. Robin, A. (2020). Le principe d'ouverture des données de la recherche scientifique. Revue Intelligibilité du numérique, 1|2020 : https://doi.org/10.34745/numerev_1690.

La mise en œuvre de la politique européennne et nationale d'ouverture des données scientifiques « balance ainsi entre le respect de l'intérêt public qui commande la diffusion ouverte des données (diffusion) et la prise en compte des intérêts privés fondés sur le secret ou les droits de propriété intellectuelle (valorisation) »[53]. En définitive, cette accessibilité des documents administratifs au public (l'*open data*) ayant pour corollaire « la libre réutilisation de ces données »[54] dont les principes sont entérinés par des mesures législatives ainsi que le recours à l'utilisation du cloud souverain par les administrations pour le stockage des données sensibles ont permis de conforter notre position quant à l'exclusion des données des personnes morales de droit public du champ de notre étude.

7. ***Plan de l'introduction*** : À titre liminaire, il apparaît opportun d'introduire le sujet par des éléments de définitions, de contexte et de dresser le panorama législatif (Section 1) avant d'exposer l'approche et la méthodologie retenues pour étudier ce sujet de thèse (Section 2).

## Section 1 : Le champ d'étude de la protection des données dans les contrats de cloud computing

8. **Plan.** Il est proposé, dans cette partie, de déterminer les données étudiées (I) et le contrat de cloud computing (II).

### I) L'étude des données

9. **Plan.** Il est envisagé d'identifier les types de données (A) et la réglementation applicable à celles-ci (B).

[53] Robin A., L'ouverture des données publiques scientifiques : de l'examen de la règle « open as possible, closed as necessary », Communication Commerce électronique n° 9, Septembre 2020, étude 15.

[54] Ibid.

## A) Les catégories de données

***10. Les données à caractère personnel.*** À l'échelle nationale, l'article 2 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[55] définit les données à caractère personnel comme étant « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ». Pour déterminer si une personne est identifiable, cet article précise qu'« il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ». À l'échelle européenne, le RGPD[56] en reprenant la définition figurant dans la Directive européenne de 1995[57], énonce à l'article 4 que les données à caractère personnel correspondent à « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") » ; ce sont uniquement les données se rattachant aux personnes physiques et non aux personnes morales. Il est précisé qu'une « personne physique identifiable » est une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

***11.*** De ces définitions, il en résulte que les données à caractère personnel correspondent aux informations qui identifient ou permettent d'identifier une personne physique. Ces définitions des données à caractère personnel sont larges, car elles s'appliquent à l'égard de tout type d'informations dès lors que celles-ci puissent être rattachées directement ou indirectement à la personne physique. En effet, la notion de données à caractère personnel comprend tous types d'informations telles que les informations, informations privées, publiques, professionnelles ou commerciales, informations objectives ou subjectives[58].

---

[55] Article 2 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés laquelle définit les données à caractère personnel (dite loi informatique et libertés). V. également, définition par la CNIL (Commission Nationale de l'Informatique et des Libertés) : il s'agit de « toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement ; par exemple : un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, etc » : https://www.cnil.fr/fr/cnil-direct/question/une-donnee-caractere-personnel-cest-quoi.

[56] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, dit « RGPD » règlement général sur la protection des données).

[57] Directive européenne 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, publié au Journal officiel n° L 281 du 23/11/1995 p. 0031 – 0050.

[58] De Terwangne C. et Rosier K., Le Règlement général sur la protection des données (RGPD / GDPR), Analyse approfondie, 1re édition 2018, Larcier.

***12.*** La jurisprudence précise, concernant les données publiques (celles qui sont accessibles au public à partir des réseaux sociaux, des sites internet ou autres registres publics…), que « ce n'est pas parce que des données ont été diffusées, c'est-à-dire portées à la connaissance ou rendues accessibles à un nombre indéfini de personnes, qu'elles ne bénéficient plus d'une protection. En d'autres termes, il n'est pas question de dépouiller de toute protection des données dès lors qu'elles sont rendues publiques d'une quelconque façon, que ce soit notamment sur internet ou dans un journal »[59].

***13.*** S'agissant des données relatives à la vie professionnelle d'un individu ou à ses activités commerciales, le Tribunal de première instance de l'Union européenne a indiqué que « les noms et prénoms des fonctionnaires européens et des personnes figurant sur les listes de réserve des concours de recrutement organisés par l'Union européenne constituaient des données à caractère personnel »[60]. La jurisprudence européenne a précisé que « pour savoir si l'on est en présence de données à caractère personnel, il ne s'agit pas de déterminer si une information relève ou non de la vie privée, mais seulement d'établir si l'information se rapporte à une personne identifiée ou identifiable. Les noms et prénoms des personnes ayant participé à une réunion de travail figurant sur le procès-verbal de la réunion ont aussi été considérés comme des données à caractère personnel »[61]. En conséquence, la doctrine considère que « la liste des données à caractère personnel est donc particulièrement longue et variée. Il peut s'agir de données contenues dans un répertoire d'adresses professionnelles ou non, dans une liste de clients, d'un numéro de plaque de voiture, de données bibliographiques, de l'identification des parties, des juges et des plaideurs dans les décisions de jurisprudence, des résultats scolaires d'un élève, du numéro de compte bancaire, d'un *log*, etc. »[62]. Ensuite, il a été considéré par la doctrine que les « données *"matérielles"* portant sur des "choses", mais pouvant être reliées à des individus identifiés, comme les données d'identification d'un véhicule ou les données cadastrales, sont aussi à considérer comme des données à caractère personnel. La valeur d'une maison rattachée au patrimoine de son propriétaire ou les données de localisation géographique de taxis associées à leurs chauffeurs relèvent ainsi de la catégorie des données à caractère personnel »[63]. Les données dites « subjectives » contenant par exemple « une évaluation ou un jugement porté sur quelqu'un »[64] sont englobées dans la notion de données à caractère personnel. Concernant la

[59] CJUE, 16 décembre 2008, affaire n° C-73/07, Tietosuojavaltuutettu c. Satakunnan markkinapörssi oy et Satamedia oy.

[60] TPIUE, 7 juillet 2011, affaire n° T-161/04, Gregorio Valero Jordana c. Commission, pt 91.

[61] CJUE (GC), 29 juin 2010, affaire n° C-28/08, Commission c. The Bavarian Lager Co. Ltd, pt 86.

[62] De Terwangne C., Rosier K., Le Règlement général sur la protection des données (RGPD / GDPR), Analyse approfondie, 1re édition 2018, Larcier.

[63] V. les développements sur ces deux exemples par le Groupe 29, WP 136, préc., p. 10 et 12 ; dans De Terwangne C. et Rosier K., Le Règlement général sur la protection des données (RGPD / GDPR), Analyse approfondie, 1re édition 2018, Larcier.

[64] CJUE, 20 décembre 2017, affaire n° C-434/16, Novak, pt 34.

protection légale attachée aux données à caractère personnel, le format de la donnée n'importe pas puisque sont visés tous les éléments qui permettent d'identifier ou de rendre identifiable une personne physique[65]. La doctrine a considéré que « les données à caractère personnel peuvent prendre n'importe quelle forme, que ce soit celle d'un texte écrit, d'un graphique, d'un dessin[66], d'images ou de son[67], de données biométriques [68] ou génétiques [69] »[70].

***14. Les données sensibles.*** Les données à caractère personnel englobent également des catégories particulières de données, telles que les données dites « sensibles »[71] ; il s'agit de données « qui font apparaître l'origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique, les données génétiques, les données biométriques, les données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique »[72]. Ainsi, les données biométriques font partie de la catégorie des données sensibles et sont définies légalement comme étant les données « résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, tel que des images faciales ou des données dactyloscopiques »[73]. Concernant la biométrie, Madame Ceyhan la définit comme étant « une technologie d'identification qui consiste à transformer une caractéristique morphologique

---

[65] Article 2 de la loi informatique et libertés et article 4 du RGPD. Exemple : il peut s'agir d'images (photographies, tableau, dessins), de vidéos (enregistrements de vidéosurveillance), de sons (échantillons de la voix), d'une partie du corps (empreinte digitale, rétinienne ou veineuse).

[66] Groupe 29, Avis 4/2007 sur le concept de données à caractère personnel : « À la suite d'un test neuropsychiatrique pratiqué sur une fillette dans le contexte d'une procédure judiciaire concernant sa garde, celle-ci fait un dessin représentant sa famille. Ce dessin fournit des informations sur l'état d'esprit de la fillette et ses sentiments envers différents membres de sa famille. Ces informations pourraient, en soi, être considérées comme des "informations à caractère personnel". Ce dessin révèle, en effet, des informations concernant cet enfant (sa santé mentale), mais aussi le comportement de son père ou de sa mère par exemple. En conséquence, les parents peuvent dans ce cas user de leur droit d'accéder à cet élément d'information spécifique » ; dans De Terwangne C. et Rosier K., Le Règlement général sur la protection des données (RGPD / GDPR), Analyse approfondie, 1re édition 2018, Larcier

[67] « En ce qui concerne les services bancaires par téléphone, où la voix du client qui donne des instructions à la banque est enregistrée, il y a lieu de considérer ces instructions enregistrées comme des données à caractère personnel », Groupe 29, Avis 4/2007 sur le concept de données à caractère personnel, p. 9 ; dans De Terwangne C. et Rosier K., Le Règlement général sur la protection des données (RGPD / GDPR), Analyse approfondie, 1re édition 2018, Larcier

[68] Groupe 29, Document de travail sur la biométrie, WP 80, 1er août 2003. V. également article 4 alinéa 14 du RGPD concernant la définition des données biométriques : les « données biométriques » sont les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

[69] Définition, les données génétiques sont « les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question » : Article 4 alinéa 13 du RGPD.

[70] De Terwangne C., Rosier K., Le Règlement général sur la protection des données (RGPD / GDPR), Analyse approfondie, 1re édition 2018, Larcier.

[71] Art. 6 de la Loi informatique et libertés (loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés laquelle définit les données à caractère personnel).

[72] Art. 9 al. 1 du RGPD.

[73] Art. 4 al.14 du RGPD.

ou comportementale en une empreinte numérique. Son objectif est d'attester l'unicité d'une personne à partir de la mesure d'une partie inchangeable et immaîtrisable de son corps »[74]. Afin de pouvoir employer un dispositif d'identification ou d'authentification biométriques sur certaines caractéristiques (empreinte digitale, analyse de la rétine, de la main ou du visage) encore faut-il veiller à ce que certaines exigences soient remplies et particulièrement, « elles doivent être uniques, universelles, permanentes et mesurables[75]. À l'intérieur de cette catégorie de données sensibles figure les données de santé qui sont définies comme étant "les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne[76]. Concernant cette catégorie particulière de données à caractère personnel, « les données sensibles », le traitement est en principe interdit sauf exceptions [77] prévues par les textes. L'alinéa 2 de l'article 9 précise ces exceptions, lesquelles sont, par exemple, le consentement explicite de la personne au traitement de ces données pour une ou plusieurs finalités spécifiques, le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée (..).

***15.*** Il en résulte que ces définitions relatives à la détermination des données à caractère personnel sont volontairement larges afin d'étendre au maximum la protection consacrée par les textes[78] et en particulier par le RGPD[79].

***16. Les données des personnes morales de droit privé***. Les données des personnes morales de droit privé font partie de la grande catégorie des données à caractère non personnel qui englobent toutes les données qui n'identifient pas ou ne permettent pas d'identifier une personne physique. Dans cette étude, les données des personnes morales englobent les informations confidentielles de l'entité telles que son exploitation, ses informations financières, ses stratégies sur le marché, ses actions de marketing, ses portefeuilles clients et fournisseurs (volume de vente, prix, marge, identité des clients). Les données stratégiques de l'entreprise sont définies comme un étant « un

[74] Ceyhan A., communication de la définition lors du Séminaire IHEJ/Esprit du 20 mars 2006, Antoine Garapon et Michaël Foessel.

[75] Debet A., Massot J. et Métallinos N., Informatique et libertés : la protection des données à caractère personnel en droit français et européen, Lextenso, 2015. V. également, article 25 de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui soumet le traitement des données biométriques à une autorisation préalable de la CNIL.

[76] Art. 4 al.15 du RGPD. V. également directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers

[77] Les Art. 6 de la Loi informatique et libertés et art. 9 al. 1 du RGPD posent le principe d'interdiction de traitement des données sensibles sauf exceptions prévues par les textes.

[78] V. thèse de Coulibaly I., La protection des données à caractère personnel dans le domaine de la recherche scientifique, Université de Grenoble, 2011. Egalement, V. thèse Le Clainche J., L'adaptation du droit des données à caractère personnel aux communications électroniques, Thèse Université de Montpellier I, 2008.

[79] RGPD : Règlement général sur la protection des données.

ensemble d'informations qui si elles étaient détenues ou mises en corrélation par des tiers pourraient permettre de prendre de vitesse ou neutraliser une prise de position envisagée par l'entreprise et dont l'impact serait d'une telle ampleur, que la stratégie de l'entreprise serait fortement ou durablement impactée (..) Par ailleurs, le caractère stratégique d'une donnée est lié à la durée de validité de l'axe stratégique de l'entreprise (fusion, appel d'offres..). Une donnée stratégique peut alors être confidentielle ou sensible pendant un temps déterminé et perdre cette caractéristique ultérieurement »[80]. L'information est « considérée comme confidentielle qu'à une triple condition : l'information ne doit pas être connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur secteur d'activité, elle doit revêtir une valeur commerciale effective ou potentielle du fait de son caractère secret, et elle doit avoir fait l'objet de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret »[81]. Aujourd'hui, ces informations confidentielles ou sensibles de la personne morale de droit privé peuvent être regroupées dans ce que l'on appelle « le patrimoine informationnel de l'entreprise » qui a été défini comme étant « l'ensemble des données, protégées ou non, valorisables ou historiques, d'une personne physique ou morale » [82] disposant « d'une valeur économique ou un intérêt stratégique, indépendamment du caractère protégeable ou non de ces informations par un droit de propriété intellectuelle »[83] et correspond à « l'universalité des données détenues et produites par une personne physique ou morale, composante de son patrimoine immatériel. Il s'agit, donc, d'un ensemble de droits et de devoirs, d'actifs et de passifs, en mutation permanente en fonction des événements juridiques de la vie numérique d'une donnée »[84]. Les données des personnes morales sont considérées comme étant des données à caractère non personnel. Au niveau européen, le RGPD ne s'applique pas au transfert des données à caractère non personnel ; c'est le règlement européen dit RDNP du 14 novembre 2018 qui s'applique[85]. Celui-ci établit un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne.

[80] CIGREF, IFACI, AFAI, Guide pratique- cloud computing et la protection des données.

[81] Robin, A. (2020). Le principe d'ouverture des données de la recherche scientifique. Revue Intelligibilité du numérique, 1l2020 : https://doi.org/10.34745/numerev_1690.

[82] Livre blanc du CIGREF (Club informatique des grandes entreprises françaises), en partenariat avec la FedISA (Fédération de l'ILM, du stockage et de l'archivage), Protection du patrimoine informationnel, publié le 30 novembre 2007, définition du patrimoine informationnel. V. également, Syntec informatique, Le Livre blanc du cloud computing, tout ce que vous devez savoir sur l'informatique dans le nuage, 2e trimestre 2010, disponible sur https://www.celge.fr/wp-content/uploads/2014/11/Syntec-informatique-cloud.pdf.

[83] Galloux J.-C., Ebauche d'une définition juridique de l'information, 1994, Dalloz chronique pp. 229-234.

[84] Saint-Aubin Th., les nouveaux enjeux juridiques des données (big data, web sémantique et linked data) Les droits de l'opérateur de données sur son patrimoine numérique informationnel, Revue Lamy Droit de l'Immatériel, N° 102, 1er mars 2014.

[85] Règlement (UE) numéro 2018/1807 du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne dit RDNP.

***17.*** Après avoir déterminé les catégories de données objet du champ d'études, il s'agit d'envisager quelle est la réglementation applicable à l'étude de la protection des données dans les contrats de cloud computing.

## B) La réglementation applicable

***18. La nécessaire identification de la réglementation applicable.*** Les personnes désirant opter pour un service de cloud computing doivent identifier en amont la réglementation applicable à leur contrat de cloud computing et évaluer la nature des risques portés à la protection de leurs données numériques. Certains auteurs ont alerté sur ces risques et ont préconisé des mises en garde en considérant la nécessité de mettre en place un régime de protection qui implique notamment des outils juridiques et légaux[86]. Qu'il s'agisse d'une réglementation nationale ou régionale[87], il est pertinent de s'interroger si l'arsenal législatif et réglementaire est suffisamment adapté à l'impératif de protection des données dans les contrats de cloud computing. La réglementation applicable au contrat de cloud computing sera fonction du type de donnée concerné qu'il s'agisse des données à caractère personnel ou des données à caractère non personnel.

***19. La réglementation applicable aux données à caractère personnel.*** En raison du développement des technologies informatiques et de l'intérêt pour le marché de la « data »[88], l'Union européenne a produit des textes pour adapter la réglementation aux nouvelles réalités du numérique et ainsi permettre une harmonisation transnationale en vue de la construction d'un « digital single market » ou « marché unique numérique »[89]. L'objectif est, d'une part, de protéger les données à caractère personnel et, d'autre part, de favoriser l'économie de la « data ».

---

[86] Eynard J., Les données personnelles, quelle définition pour un régime de protection efficace ? Michalon Editeur, 2013 : « À l'heure du tout numérique, la protection des données personnelles est devenue un enjeu majeur. Parce qu'elles échappent à la maîtrise de l'individu qu'elles concernent, il est aujourd'hui essentiel de mettre en place un régime de protection qui implique des acteurs professionnels capables de proposer des outils (juridiques, légaux et techniques) efficaces pour assurer une protection optimale ».

[87] V. Castets-Renard C., Droit de l'internet : droit français et européen, Montchrestien, Lextenso éditions, 2018.

[88] Traduction : Marché de la « donnée ».

[89] Castets-Renard C, Droit du marché unique numérique et intelligence artificielle, Préface de Picod F., édition Bruylant, collection droit de l'union européenne, novembre 2020 : « Le marché unique numérique, tel que présenté par la Commission européenne dans sa Stratégie du 6 mai 2015 (COM [2015] 192 final), peut paraître comme une simple extension à l'environnement numérique du marché intérieur. En réalité, sa portée est bien plus importante, dans la mesure où il concerne la régulation des contenus, l'utilisation des technologies pour faciliter les échanges internes et externes à l'Union, mais aussi les infrastructures nécessaires au développement des technologies du numérique ». V. également, Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (dit « RGPD » règlement général sur la protection des données).

***20.*** Au niveau européen, dès lors que les données stockées dans le cloud computing concernent des données à caractère personnel, lesquelles font l'objet d'une collecte et d'un traitement, le RGPD (règlement général sur la protection des données)[90] abrogeant la directive 95/46/CE, a vocation à s'appliquer. À la suite de l'entrée en vigueur du RGPD, la France a modifié sa réglementation relative à la protection des données à caractère personnel ; en particulier la loi du 6 janvier 1978 dite loi informatique et libertés pour intégrer les apports du RGPD par la loi numéro 2018-493 du 20 juin 2018 relative à la protection des données personnelles, puis du décret numéro 2018-687 du 1er août 2018 et de l'ordonnance numéro 2018-1125 du 12 décembre 2018[91].Tel que rappelé par certains auteurs, le RGPD « ne bouleverse pas tant le droit existant en raison de son contenu : nombre des règles qu'il contient existaient déjà. Il en change davantage la philosophie, en optant pour une responsabilisation des acteurs tout au long des traitements de données, et en renforce considérablement les sanctions »[92]. Cette réglementation étant générale, des réglementations spécifiques pour la protection des données à caractère personnel dans des domaines particuliers ont été produites ; on parle alors de réglementations sectorielles telles que celle relative à la protection des données en matière pénale et en matière de santé adoptée en France, avec la loi du 20 juin 2018 [93] et au niveau de l'Union européenne, avec la Directive de l'Union européenne du 27 avril 2016 dite « Directive Police-Justice » [94] laquelle a pour champ d'application la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces et la libre circulation de ces données. Il sera, notamment, abordé, la question de savoir si la réglementation applicable à la protection des données à caractère personnel dans les contrats de cloud computing est efficace dans un environnement globalisé.

---

[90] RGPD.

[91] Modification de la loi numéro 78-17 du 6 janvier 1978 informatique, V. loi numéro 2018-493 du 20 juin 2018 relative à la protection des données personnelles, V. décret numéro 2018-687 du 1er août et V. ordonnance numéro 2018-1125 du 12 décembre 2018.

[92] Perray R. et Rochfeld J., Les défis sectoriels du RGPD, Anonymisation, véhicules autonomes, eSanté, FinTechs, smart cities, AI et concurrence, édition LexisNexis, septembre 2019. V. également, Ragheno N., Data Protection & Privacy, Le GDPR dans la pratique / De GDPR in de praktijk, Revue de droit international et de droit comparé, 14 juin2018, numéro 2, page(s) 307-310.

[93] Adoption en France de la loi numéro 2018-493 du 20 juin 2018 publiée au JORF n°0141 du 21 juin 2018 relative à la protection des données personnelles qui intègrent les dispositions concernant la protection des données en matière pénale et en matière de santé.

[94] Adoption de la Directive européenne numéro 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la Matière ou d'exécution de sanctions pénales et à la libre circulation de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil. V. également, application de la Directive numéro 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers publiée au JO L88 du 4.4.2011, p.45. V. Munari Y., L'apport du droit de l'union européenne en droit des contrats internationaux de cloud computing, Mémoire de master 2 droit européen des affaires, sous la direction de Mme Blandine de Clavière Professeur à l'Université Jean Moulin Lyon 3, soutenu à Lyon, le 13 juillet 2016.

***21.*** La réglementation protectrice des données à caractère personnel est étudiée, au niveau internaitonal, et en particulier celle des États-Unis. Au niveau fédéral des États-Unis, il est observé l'absence d'une réglementation générale protectrice des données à caractère personnel. En revanche, il existe des réglementations sectorielles telles que « the United States Privacy Act » qui est une loi sur la protection de la vie privée adoptée en 1974 établissant un code de pratiques équitables en matière d'information qui régit la collecte, la conservation, l'utilisation et la diffusion d'informations sur les individus, lesquels sont conservées dans des systèmes d'enregistrement par les agences fédérales. Ce texte exige que les agences informent le public de leurs systèmes d'enregistrement en les publiant dans le registre fédéral (« Federal Register »). Cette loi interdit la divulgation d'un dossier concernant un individu à partir d'un système de dossiers sans le consentement écrit de l'individu, sauf si la divulgation est conforme à une exception légale. La loi fournit également aux individus un moyen de demander l'accès et la modification de leurs dossiers, et énonce diverses exigences en matière de tenue de dossiers. Également, « the Health Insurance Portability and « Accountability Act (HIPAA)» est une loi fédérale de 1996 sur la portabilité et la responsabilité en matière d'assurance maladie qui intègrent des dispositions relatives à la simplification administrative, en particulier pour l'adoption de normes nationales pour les transactions de soins de santé électroniques et les jeux de codes, les identificateurs de santé uniques et la sécurité. Par la suite, cette loi a été modifiée en 2002 et en 2003 pour préserver la confidentialité des informations de santé et intègre des dispositions rendant obligatoire l'adoption de mesures fédérales de protection de la vie privée pour les informations sanitaires rendant identifiables les individus. Il existe, également, des lois ad hoc telles que « The Video Privacy Protection Act of 1988 » est une loi adoptée par le Sénat le 11 mai 1988 qui modifie le code pénal fédéral afin d'interdire, à certaines exceptions près, la divulgation de dossiers de location de vidéos contenant des informations personnelles identifiables. Cette loi autorise la divulgation de ces informations au consommateur, avec le consentement écrit du consommateur, en vertu d'un mandat pénal fédéral, d'un mandat d'État équivalent, d'une citation à comparaître devant un grand jury ou d'une ordonnance du tribunal conformément à des directives spécifiques, à toute personne si cette divulgation concerne uniquement les noms et adresses des consommateurs et si le consommateur a eu la possibilité d'interdire cette divulgation, à toute personne si cette divulgation est liée au cours normal des affaires du fournisseur de services de bandes vidéo, ou en vertu d'une ordonnance du tribunal civil. Ensuite, « the Fair Credit Reporting Act » est une loi fédérale américaine adoptée le 26 octobre 1970 qui protège les informations recueillies par les agences de renseignements sur les consommateurs, telles que les agences d'évaluation du crédit, les sociétés d'information médicale et les services de vérification des locataires. Il est spécifié dans le titre VI de cette loi

que les informations contenues dans un rapport sur le consommateur ne peuvent être fournies à quiconque n'ayant pas un but spécifié par la loi. Également, il est mentionné que les entreprises qui fournissent des informations aux agences de renseignements sur les consommateurs ont également des obligations légales spécifiques, notamment le devoir d'enquêter sur les informations contestées. En outre, il est exigé des utilisateurs de ces informations à des fins de crédit, d'assurance ou d'emploi qu'ils informent le consommateur lorsqu'une mesure défavorable est prise sur la base de ces rapports. Lesdites lois ne sont que des lois prises dans des secteurs déterminés et n'ont pas vocation à régir de manière générale la protection des données à caractère personnel. En revanche, il a été observé que certains États fédérés ont adopté des lois pour la protection des données des consommateurs. À titre d'exemple, l'état de Californie a adopté le 28 juin 2018, une loi pour la protection de la vie privée des consommateurs, le "California Consumer Privacy Act (CCPA) of 2018 ". Cette loi intègre des dispositions relatives à la protection des données à caractère personnel du consommateur et accorde aux consommateurs davantage de contrôle sur les informations personnelles que les entreprises collectent à leur sujet. Plus particulièrement, cette loi garantit de nouveaux droits à la vie privée pour les consommateurs californiens, notamment le droit de connaître les informations personnelles qu'une entreprise collecte à leur sujet et la manière dont elles sont utilisées et partagées, le droit de supprimer les informations personnelles recueillies à leur sujet (avec quelques exceptions), le droit de refuser la vente de leurs informations personnelles et le droit à la non-discrimination dans l'exercice de leurs droits. Cette loi s'applique à de nombreuses entreprises, y compris les courtiers en données dans le territoire de la Californie.

22. ***La réglementation applicable aux données des personnes morales de droit privé.*** La réglementation protectrice du RGPD n'a pas vocation à s'appliquer aux données de la personne morale de droit privé. Le RGPD affirme expressément que : « le présent règlement ne couvre pas le traitement des données à caractère personnel qui concerne les personnes morales, et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale »[95]. Il n'existe pas pour l'heure de réglementation spécifique à la protection des données des personnes morales qui serait équivalente à celle applicable aux personnes physiques. Ainsi, en France, les données des personnes morales sont protégées non pas par une réglementation spécifique, mais par le régime de droit commun de la responsabilité civile et pénale, le régime spécial de la propriété

[95] Considérant 14 du RGPD.

intellectuelle et le régime du secret des affaires[96]. Au niveau européen, prenant conscience de ce vide juridique, des textes ont été adoptés. En matière de protection des données et des communications en ligne, il a été adopté en 2002, une Directive européenne dite « directive vie privée et communications électroniques » laquelle vise à protéger les données et la confidentialité des communications en ligne [97]. L'Union européenne a entamé une réflexion sur la construction d'un marché unique de la donnée. À ce titre, la communication intitulée « stratégie pour un marché unique numérique en Europe », publiée en 2015, pointait déjà que la fragmentation des réglementations entre les États constituait le principal obstacle à la croissance des entreprises européennes du numérique. En 2016, il a été adopté une Directive européenne relative à la protection du savoir-faire et des informations commerciales non divulguées contre l'obtention, l'utilisation et la divulgation illicites[98]. Puis, il a été adopté en 2018 un Règlement européen lequel établit un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne au sein de l'Union européenne [99] ce règlement a été suivi deux propositions de règlements lesquels ont été adoptés et sont présentés ci-après.

***23.*** La proposition de règlement dite DMA[100] (*Digital Market Act*) a pour objet d'établir « des règles harmonisées visant à garantir la contestabilité et l'équité des marchés dans le secteur numérique de l'Union là où des contrôleurs d'accès sont présents sur le marché »[101]. Il s'agit de développer un marché numérique européen équitable, sûr, responsable et ouvert. Cette proposition a fait l'objet, le 24 mars 2022, d'un accord politique provisoire entre le Conseil et le Parlement puis a été adoptée le 14 septembre 2022[102]. Le DMA a été publié au Journal officiel de l'UE le 12

---

[96] Adoption de la loi du 30 juillet 2018 relative à la protection du secret des affaires et son décret du 11 décembre 2018 transposant la directive 2016/943 de l'Union européenne du 8 juin 2016 sur la protection du savoir-faire et des informations commerciales non divulguées contre l'obtention, l'utilisation et la divulgation illicites.

[97] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Cette Directive est en cours de révision et va laisser place, en cas d'adoption, au Règlement E.privacy du Parlement européen et du Conseil dont la proposition été publiée le 10 janvier 2017 et est toujours en cours de négociation. Non encore adopté, le règlement « vie privée et communications électroniques » ou le règlement E.Privacy concerne le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques. Il vise à compléter les règles générales de protection des données à caractère personnel définies dans le RGPD concernant les données de communications électroniques. Ce projet de règlement se veut d'une application large puisqu'il a vocation à s'appliquer à tous les moyens de communication actuels et futurs (téléphonie vocale, accès à internet, les applications de messagerie instantanée, le courrier électronique, les appels téléphoniques par Internet et la messagerie personnelle fournie par les réseaux sociaux).

[98] Directive 2016/943 de l'Union européenne du 8 juin 2016 sur la protection du savoir-faire et des informations commerciales non divulguées contre l'obtention, l'utilisation et la divulgation illicites

[99] Règlement (UE) numéro 2018/1807 du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne applicable depuis le 19 avril 2019. Ce texte a pour objet d'établir les règles en matière de transfert de données à caractère non personnel (celles qui ne concernent pas « une personne physique identifiée ou identifiable » et celles qui « étaient initialement des données à caractère personnel, mais qui ont ensuite été rendues anonymes ») et le principe consacré est la libre circulation des données au sein de l'Union européenne.

[100] Proposition de Règlement du parlement européen et du conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques),15 décembre 2020, COM(2020) 842 final.

[101] Article 1er du DMA.

[102] Conseil de l'UE, communiqué de presse « Législation sur les marchés numériques (DMA) : accord entre le Conseil et le Parlement européen », 25 mars 2022. Règlement 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux

octobre 2022, entrera en vigueur le 1er novembre 2022 et sera applicable à partir du 2 mai 2023. Ce texte s'applique à des contrôleurs d'accès qui fournissent ou proposent des services de plateforme essentiels à des entreprises utilisatrices établies dans l'Union ou aux utilisateurs finaux établis ou situés dans l'Union, quel que soit le lieu d'établissement ou de résidence des contrôleurs d'accès et quel que soit le droit par ailleurs applicable à la fourniture des services[103]. La question se pose de savoir si ce texte concerne les services de cloud computing. La réponse nous est fournie à l'article 2, 2, g du texte qui indique que les services de plateforme essentiels recouvrent, notamment, les services d'informatique en nuage fournis par un fournisseur de services de plateforme,[104] lequel est désigné comme contrôleur d'accès si: « (a) il a un poids important sur le marché intérieur ; (b) il assure un service de plateforme essentiel qui constitue un point d'accès majeur permettant aux entreprises utilisatrices d'atteindre leurs utilisateurs finaux; et (c)il jouit d'une position solide et durable dans ses activités ou jouira, selon toute probabilité, d'une telle position dans un avenir proche»[105]. Des critères sont, ainsi, établis. Une plateforme est définie comme « contrôleur d'accès » si l'entreprise a réalisé un chiffre d'affaires annuel dans l'EEE supérieur ou égal à 6 500 000 000 EUR au cours des trois derniers exercices, ou si la capitalisation boursière moyenne ou la juste valeur marchande équivalente de l'entreprise atteint au moins 65 000 000 000 EUR au cours du dernier exercice, et qu'il fournit un service de plateforme essentiel dans au moins trois États membres[106] ; ou « s'il fournit un service de plateforme essentiel qui a enregistré plus de 45 millions d'utilisateurs finaux actifs par mois établis ou situés dans l'Union et plus de 10 000 entreprises utilisatrices actives par an établies dans l'Union au cours du dernier exercice »[107]. Ce qui signifie que ce texte ne concerne pas toute les entreprises, mais uniquement l'entreprise qui a une position économique forte sur le marché. En définitive, une entreprise prestataire de services cloud répondant à ces critères devra s'identifier comme contrôleurs d'accès auprès de la Commission[108], qui pourra dans le cas contraire procéder à des enquêtes pour les identifier. Par ailleurs, ce texte bénéficie aux utilisateurs finaux (consommateurs) et aux entreprises utilisatrices (considérant 14). Les obligations incombant au contrôleur d'accès sont énoncées à l'article 5 à 8 et sont relatives aux pratiques des contrôleurs d'accès qui limitent la contestabilité ou sont déloyales. Parmi les

---

marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques).

[103] Article 1er du DMA.

[104] Article 2, 1 du DMA.

[105] Article 3 du DSA.

[106] Article 3, 2, a du DSA.

[107] Article 3, 2, b du DSA.

[108] Article 3, 3 du DSA.

obligations en lien avec le sujet étudié, il y a celles relatives à l'utilisation, à la portabilité des données (art.6) et à l'obligation de fournir gratuitement des interfaces techniques qui facilitent l'interopérabilité (art.7). Ces règles visent à créer un marché en ligne équitable, et prévoit des amendes élevées en cas de non-respect du DMA pouvant atteindre 10% du chiffre d'affaires total de l'année précédente.

***24.*** Puis, quant à la proposition dite DSA (Digital Service Act) du 15 décembre 2020[109], elle a pour objectif de rénover le droit applicable aux intermédiaires techniques et vise à « (a) contribuer au bon fonctionnement du marché intérieur des services intermédiaires ; (b) établir des règles uniformes pour un environnement en ligne sûr, prévisible et digne de confiance, dans lequel les droits fondamentaux consacrés par la Charte sont efficacement protégés »[110]. Cette proposition a fait l'objet, le 23 avril 2022, d'un accord politique provisoire entre le Conseil et le Parlement, puis d'une vote par le Parlement européen le 5 juillet et d'une adoption par le Conseil de l'UE le 4 octobre 2022[111]. Le DSA du 19 octobre 2022[112] devrait entrer en application dans les quinze mois après l'entrée en vigueur ou le 1er janvier 2024 (article 93), sauf pour les très grandes plateformes en ligne et les très grands moteurs de recherche qui devront connaître une application anticipée de ce texte (Article 92). Ce texte instaure un mécanisme permettant aux utilisateurs de signaler ces contenus et aux plateformes de coopérer avec des signaleurs de confiance[113]. Ce texte s'applique aux services intermédiaires fournis aux bénéficiaires du service dont le lieu d'établissement ou de résidence se situe dans l'Union, quel que soit le lieu d'établissement des fournisseurs de ces services. Les services intermédiaires sont définis à l'article 2 du DSA et les prestations de services cloud en font partie[114]. Le DSA institue l'obligation pour les plateformes en ligne de retirer *« promptement »* tout contenu illicite dès qu'elle en a connaissance, l'instauration d'une procédure de notification permettant aux utilisateurs de signaler du contenu illicite en ligne, un renforcement des informations fournies par les vendeurs (obligation désignée sous la dénomination « Know Your Business Customer), des signaleurs de confiance faisant le lien entre les victimes de ces contenus et les plateformes

[109] Proposition de Règlement du parlement européen et du conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE, du 15 décembre 2020, COM (2020) 825 final.

[110] Article 1 du DSA.

[111] Conseil de l'UE, communiqué de presse « Législation sur les services numériques : accord provisoire du Conseil et du Parlement européen pour faire d'internet un espace plus sûr pour les citoyens européens », 23 avril 2022.

[112] Règlement (UE) 2022/2065 du parlement européen et du conseil, du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).

[113] Bertrand B., La confiance numérique, Chronique Droit européen du numérique, RTD Eur. 2021 p.153.

[114] Article 2, f du DSA : « service intermédiaire », un des services suivants : (...) –un service d'« hébergement» consistant à stocker des informations fournies par un bénéficiaire du service à la demande de ce dernier ».

pour signaler du contenu illicite. Le statut de « signaleur de confiance »[115], ne peut être octroyé qu'à des personnes morales qui ont une expertise particulière dans la lutte contre les contenus illicites, qui représentent des intérêts collectifs et travaillent de manière diligente et objective (Art.19, DSA)[116]. Ce statut est révocable[117].

***25.*** Après avoir déterminé le champ d'étude des données et dressé le panorama législatif et réglementaire, il convient d'étudier le contrat de cloud computing.

## II) L'étude du contrat de cloud computing

**Plan.** Pour étudier la protection des données dans les contrats de cloud computing, il est nécessaire de déterminer ce qu'est le « cloud computing » (A) avant d'étudier précisément les contrats de cloud computing (B).

### A) Le cloud computing

***26.*** Historiquement, le premier acteur à avoir fait une offre de service au public, c'est Amazon. Cette offre de service cloud avait pour objet de proposer aux entreprises de louer une partie des capacités informatiques (data centers) d'Amazon. La spécificité, ici, c'est que la location était rendue possible par l'établissement d'une connexion Internet sécurisée entre le client et Amazon en qualité de fournisseur de ressources cloud. C'est ainsi que « Amazon Web Services » (AWS) est apparu et est devenu le premier acteur leader sur le marché des services de cloud computing pour les entreprises. Ensuite, c'est Google qui emboîte le pas avec des Services de cloud computing pour les particuliers avec Gmail. Aujourd'hui, l'offre de cloud computing s'est généralisée en ciblant une clientèle de professionnels (Business to Business) et de particuliers (Business to Consumer).

***27.*** Deux approches peuvent être entreprises pour définir le cloud computing. La première est d'envisager le cloud computing à travers le prisme purement « technologique » puis la seconde

[115] Conditions pour être signaleur de confiance : « Ce statut est accordé par le coordinateur national des services numériques, à la demande de toute entité qui remplit trois conditions cumulatives : il doit disposer d'une expertise et d'une compétence particulières pour la détection, l'identification et la notification des contenus illicites ; il doit représenter des intérêts collectifs et être indépendant de toute plateforme numérique ; il doit, enfin, soumettre des notifications en temps utile, avec diligence et objectivité : Bertrand B., La confiance numérique, Chronique Droit européen du numérique, RTD Eur. 2021 p.153.

[116] Art. 19 du DSA indique que les plateformes en ligne doivent prendre les mesures techniques et organisationnelles nécessaires pour garantir que les avis soumis par des signaleurs de confiance fassent l'objet d'une décision prioritaire sans délai.

[117] Précision sur le statut : « Le coordinateur des services numériques qui a accordé le statut de signaleur de confiance à une entité doit révoquer ce statut s'il détermine, à la suite d'une enquête menée soit de sa propre initiative, soit sur la base d'informations reçues par des tiers, y compris les informations fournies par une plateforme en ligne, que l'entité ne remplit plus les conditions » : Bertrand B., La confiance numérique, Chronique Droit européen du numérique, RTD Eur. 2021 p.153.

est de l'appréhender du point de vue du juriste et de tenter d'aboutir à une définition juridique qui aujourd'hui fait défaut.

***28.*** En technologie, le cloud computing ou « informatique en nuage »[118] ou « infonuage » ou « nébulique »[119], est décrit, avec aisance par les professionnels de l'informatique en nuage, comme « un accès via un réseau de télécommunications, à la demande et en libre-service, à des ressources informatiques partagées et stockées dans des serveurs »[120]. Il s'agit, ainsi, d'une technologie qui exploite la puissance de calcul ou de stockage de serveurs informatiques, lesquels sont distants et connectés entre eux par un réseau internet[121]. Concrètement, cette technologie permet aux utilisateurs d'accéder à des ressources stockées dans un serveur « distant » par le biais de l'utilisation d'un terminal (un ordinateur, un téléphone portable, une tablette) et de mutualiser, ainsi, une infrastructure informatique[122]. Un rapport de l'Université de Californie à Berkeley résumait les caractéristiques clés de l'informatique en nuage comme suit : « l'illusion de ressources informatiques infinies ; l'élimination d'un engagement initial des utilisateurs de l'informatique en nuage ; et la capacité de payer pour l'utilisation […] au besoin […] »[123]. Une autre définition est proposée qui consiste à présenter l'informatique en nuage comme étant « un modèle de traitement de l'information dans le cadre duquel des capacités informatiques centralisées sont fournies sous forme de services, au besoin, sur l'ensemble du réseau à une variété d'appareils destinés aux utilisateurs »[124]. Tel qu'affirmé par certains auteurs, « l'informatique en nuage est le dernier paradigme qui consiste à offrir des services hébergés sur

---

[118] Traduction officielle « du cloud computing » : Avis de la Commission Générale de Terminologie et de Néologie, Vocabulaire de l'informatique et de l'internet publié au JO le 6 juin 2010, p.10453

[119] Selon l'expression de Gaudrat Ph. et Sardain F., Traité de droit civil du numérique, t.2, Larcier, 2015, n°578 s. V. également, Le Tourneau Ph., Contrats du numérique, informatiques et électroniques, Dalloz, 12e édition, 2022-2023.

[120] Traduction personnelle réalisée à partir de la définition du cloud computing du National Institute of Standards and Technology: « Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models ». V. article « NIST défininition of cloud computing, US department of commerce, special publication 800-145, septembre 2011. http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf. V. également, thèse de Medhioub H., Architectures et mécanismes de fédération dans les environnements Cloud Computing et Cloud Networking, Telecom Sudparis et l'Université Pierre et Marie Curie, 28 avril 2015.

[121] Concernant l'identification du cloud computing : thèse de Medhioub H., Architectures et mécanismes de fédération dans les environnements Cloud Computing et Cloud Networking, Telecom Sudparis et l'Université Pierre et Marie Curie, 28 avril 2015.

[122] Également, les traits caractéristiques du Cloud sont l'externalisation des ressources, la délocalisation de l'infrastructure informatique, une grande capacité de stockage, une disponibilité mondiale et quasi-immédiate des ressources stockées, une accessibilité sur différents types d'appareils et une facturation qui se fait à la demande en fonction de la capacité de stockage utilisée : Red Hat, Cloud computing, Une infrastructure informatique, qu'est-ce que c'est ? https://www.redhat.com/fr/topics/cloud-computing/what-is-it-infrastructure.

[123] Traduction personnelle réalisée à partir de la citation suivante: "A report from the University of California Berkeley summarized the key characteristics of cloud computing as: "the illusion of infinite computing resources; (2) the elimination of an up-front commitment by cloud users; and the ability to pay for use … as needed..." : Buyya R., Broberg J., et Goscinski A.M, Cloud Computing : Principles and Paradigms, John Wiley & Sons, 2010.

[124] Traduction personnelle réalisée à partir de la citation suivante: « Cloud computing is an information-processing model in which centrally administered computing capabilities are delivered as services, on an as-needed basis, across the network to a variety of user-facing devices » : Chee B. et Franklin C. Jr, Cloud Computing: Technologies and Strategies of the Ubiquitous Data Center, CRC Press, 2010

internet, selon une approche de paiement à l'utilisation. Il permet de fournir divers services aux entreprises et aux clients, personnes physiques »[125].

***29.*** Du point de vue du juriste, lorsqu'il s'agit d'appréhender et de définir le cloud computing, la tâche s'avère plus délicate. Dans le dictionnaire juridique, le cloud computing est défini comme étant « une technologie d'externalisation des logiciels et des données informatiques (habituellement stockés dans l'entreprise) au profit d'un sous-traitant »[126]. L'expression « cloud computing » fait directement référence « au caractère nébuleux de ses pratiques »[127] et particulièrement lors de la réalisation de la prestation informatique. Selon la Commission générale de terminologie et de néologie, le cloud computing est un « mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire »[128]. Dans ce sens, le cloud computing correspond à « une forme particulière de gérance de l'informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance du client »[129]. Malgré ce travail de définitions du cloud computing, celles-ci n'embrassent pas toutes les fonctionnalités que peut revêtir aujourd'hui le cloud computing. En effet, en tant qu'objet immatériel, la détermination juridique du cloud computing requiert un effort intellectuel bouleversant les règles classiques de qualifications analytiques, tant l'objet est complexe à identifier et à définir d'un seul trait en raison de ces différents types de prestations de services cloud proposés en pratique.

***30.*** Il convient d'appréhender la figure contractuelle du contrat de cloud computing laquelle a connu un développement considérable depuis une vingtaine d'années.

---

[125] Traduction personnelle réalisée à partir de la citation suivante: "Cloud Computing is the latest paradigm that involves delivering hosted services over the Internet, based on a pay-as-you-go approach. It allows for provision of a variety of business and customer services": Mahmood Z. et Hill R., Cloud Computing for Enterprise Architectures, Springer, 2011.

[126] Guinchard S. et Débard T., Lexique des termes juridiques, Dalloz édition 2020 2021.

[127] Sordet E. et Milchoir R., Le cloud computing, un objet juridique non identifié ? Comm. Com. électr. 2011, étude n°20.

[128] Avis de la Commission Générale de Terminologie et de Néologie, Vocabulaire de l'informatique et de l'internet publié au JO 6 juin 2010, p.10453. Également, V. Alexis Baumann, dictionnaire juridique, Définition de Informatique en nuage : https://www.dictionnaire-juridique.com/definition/informatique-en-nuage.php.

[129] Définition donnée par la Commission de Terminologie et de Néologie : Avis de la Commission Générale de Terminologie et de Néologie, Vocabulaire de l'informatique et de l'internet publié au JO 6 juin 2010, p.10453

## B) Le contrat de cloud computing

***31.*** **Plan.** Le contrat de cloud computing a pour objet de déterminer les conditions dans lesquelles un prestataire, à la demande d'un client, prend en charge un service de fourniture à distance et à la demande, de ressources informatiques, infrastructures, plateformes ou logiciels d'application. Il s'agit de l'objet principal du contrat de cloud. Également, il est possible d'ajouter des prestations complémentaires de type « hébergement », « maintenance » ou autres qui forment un tout « indivisible ». En fonction de l'offre acceptée par le client, le contenu du contrat de cloud computing disposera de clauses spécifiques relatives, d'une part, à l'exécution des prestations de services de cloud computing et, d'autre part, à la politique concernant le traitement, le stockage, la disponibilité et la sécurité des données. Il est envisagé d'identifier la nature du contrat de cloud computing (1) et son origine (2).

### 1) La nature juridique du contrat de cloud computing

***32.*** La nature juridique des contrats de cloud computing a suscité un débat sur le fait de savoir si ce contrat devait recevoir la qualification de contrat de location, de contrat d'entreprise voire de contrat de dépôt. Il est considéré par certains auteurs que si certaines qualifications juridiques peuvent être évidentes « à l'instar des licences d'utilisation de logiciels SaaS ou PaaS, qui sont une catégorie particulière de contrats de location, pour d'autres, en particulier pour les prestations d'hébergement, il est possible de parler de conflit de qualifications »[130]. Ainsi, pour ces « autres contrats d'hébergement de données cloud computing », il est proposé en doctrine les qualifications de contrat de location, de dépôt ou d'entreprise.

***33.*** Le contrat de location de droit commun, appelé également, bail civil est défini à l'article 1709 du code civil comme : « un contrat par lequel l'une des parties s'oblige à faire jouir l'autre d'une chose pendant un certain temps, et moyennant un certain prix que celle-ci s'oblige de lui payer ». Pour pouvoir appliquer la qualification du contrat de location, il faudrait réunir les conditions relatives à la jouissance de la chose, une durée déterminée et le versement d'une contrepartie (le loyer) ; ensuite, la location peut porter sur un bien meuble (corporelle ou

[130] Bourgeois M., JurisClasseur Communication, Fasc. 962 : cloud computing – Les défis contractuels du Cloud Computing, 1er mai 2020.

incorporelle) ou immeuble[131]. Concernant la jouissance de la chose, elle implique que la chose soit mise à la disposition du loueur, qu'il puisse en tirer profit, et enfin qu'elle soit restituable[132].

***34.*** Ensuite, le contrat de dépôt est défini à l'article 1915 du code civil comme : « l'acte par lequel on reçoit la chose d'autrui, à la charge de la garder et de la restituer en nature ». En application de l'article 1918 du code civil, le contrat de dépôt ne peut pas porter sur des choses mobilières. À la différence du contrat de location, le dépositaire n'a pas en principe le droit de se servir de la chose : son obligation est d'en assurer la garde dans l'intérêt du déposant et non d'en jouir. Également, la distinction entre le contrat de dépôt et le contrat de location revêt un intérêt dès lors qu'une personne « remet à une autre la jouissance d'un emplacement ou d'un local pour y entreposer des biens mobiliers ». La Cour de cassation décide qu'il y a contrat de bail si le propriétaire des lieux n'assume aucune obligation de garder des objets placés dans le local. Au contraire, si la convention oblige le propriétaire des lieux à veiller à la garde de la chose, il y a dépôt. Il semblerait que « cette distinction n'est cependant pas entièrement déterminante, car un bailleur peut être tenu à une obligation d'assurer la surveillance des lieux ».

***35.*** Concernant le contrat de cloud computing, il apparaît, à première vue, que c'est la condition de « jouissance de la chose » (et donc de maîtrise) qui justifie de retenir la qualification de contrat de location. Tel qu'affirmé par Madame Bourgeois « c'est bien cette maîtrise qui distingue le contrat de location du contrat de dépôt : déposer une chose dans un lieu dont on n'est pas maître (dépôt) est juridiquement bien distinct de l'hypothèse selon laquelle on conserve des biens dans un lieu dont on détient la maîtrise (location) ; du contrat d'entreprise qui suppose la mise à disposition d'une chose, laquelle est en réalité l'accessoire d'un ensemble de prestations de services connexes (..) »[133].

***36.*** Au niveau de la doctrine, certains auteurs dont le professeur Le Tourneau rejettent la qualification de contrat de dépôt puisque selon lui « l'informatique en nuage n'est pas un dépôt, car le dépôt ne peut porter que sur un bien meuble corporel »[134]. Il considère que « le contrat permettant de loger des données dans l'espace est en principe un louage (à distance). Cependant, lorsque des prestations de services sont importantes, la qualification de louage d'ouvrage (d'entreprise) devrait être retenue »[135]. En d'autres termes, dès lors que la location à distance est assortie de prestations de services et que celles-ci apparaissent plus importantes que la location

[131] Article 1713 du code civil : « On peut louer toutes sortes de biens meubles ou immeubles ».

[132] Bénabent A, Droit des contrats spéciaux civils et commerciaux, LGDJ, 12e éd., 2017, n° 322 et s., p. 249.

[133] Bourgeois M., JurisClasseur Communication, Fasc. 962 : CLOUD COMPUTING – Les défis contractuels du Cloud Computing, 1er mai 2020 : Par exemple, l'hébergement hôtelier est moins un contrat de location, qu'un contrat de prestations de services hôteliers, puisque le client ne disposera d'aucune maîtrise sur sa chambre.

[134] Le Tourneau Ph., Contrats du numérique, informatiques et électroniques, Dalloz, 12e édition 2022/2023.

[135] Ibid.

alors la qualification de louage d'ouvrage (contrat d'entreprise) s'impose [136]. À ce titre, c'est l'article 1710 du code civil qui définit le contrat de prestation de services (louage d'ouvrage) comme : « (..) un contrat par lequel l'une des parties s'engage à faire quelque chose pour l'autre, moyennant un prix convenu entre elles ». Au vu de cette position doctrinale, la question se pose, donc, de savoir si le contrat de cloud computing ne serait pas une nouvelle application du contrat d'entreprise ? Pour apporter des éléments de réponse, il faut se demander au préalable à quoi s'oblige le prestataire. Est-ce que le prestataire s'est engagé à réaliser un ouvrage ? En cas de réponse affirmative à cette question, il faut dans ce cas identifier les caractéristiques de cet ouvrage. Concernant la réalisation de cet ouvrage, selon Ph. Gaudrat et F. Sardain, « consiste-t-elle en une réalisation particulière ou seulement à mettre à disposition à distance un outil avec lequel son client réalisera proprio motu les opérations de son choix ? Si l'objet principal de son engagement consiste à mettre à disposition un outil préexistant, il ne peut s'agir d'un contrat d'entreprise. Sans doute le contrat d'entreprise peut-il comporter une obligation de délivrance comme en l'espèce mais celle-ci ne peut avoir pour objet que la chose façonnée sur mesure au titre de l'ouvrage dû. La standardisation de l'objet mis à disposition, ce dont atteste le fait que son utilisation est largement partagée, démontre qu'il ne peut s'agir d'un contrat d'entreprise. L'obligation caractéristique telle qu'identifiée a, en revanche, tout à voir avec l'obligation de délivrance à laquelle est tenu un bailleur »[137]. Il en résulte qu'en présence d'une réalisation particulière, il est possible de présumer que l'on se trouve dans un contrat d'entreprise. Alors que s'il est question seulement de mettre à disposition un outil standard permettant à plusieurs clients d'utiliser simultanément les fonctionnalités du logiciel, il ne peut être considéré comme étant un contrat d'entreprise et devrait être considéré comme étant un contrat de location (à distance). En effet, la standardisation de l'objet mis à disposition exclut la qualification de contrat d'entreprise et par la même occasion l'obligation de résultat[138] .

***37.*** Dans une telle situation, la standardisation est reconnue dès lors que l'utilisation du logiciel est partagée simultanément par plusieurs clients différents. Aujourd'hui, la doctrine considère que « la qualification en contrat de louage de services ou contrat d'entreprise semble la mieux adaptée et la plus représentative des multiples applications des contrats de cloud »[139] puisque très souvent il est annexé à la prestation de service principale consistant en la location d'un

[136] Ibid.

[137] Gaudrat Ph. et Sardain F., Traité de droit civil du numérique, Tome 2 Droit des obligations, édition Larcier 2015, page 290, paragraphe 566.

[138] Ibid.

[139] Cette qualification est clairement, aujourd'hui, adoptée par la doctrine : Cordier G., Le contrat ASP, Comm. Com. électr.2008, n° 10, prat. 9 ; et à propos du cloud dans son ensemble ; Chantepie G., L'inexécution du contrat de cloud computing, RLDI 2013/98, p.117.

espace de stockage des données dans le cloud, des services annexes sur mesure aux clients tels que la maintenance, l'assistance par le prestataire de services cloud.

2) **L'origine du contrat de cloud computing**

***38.*** Si le cloud computing constitue une révolution économique par la mutualisation des moyens techniques, il n'en demeure pas moins qu'elle repose sur des technologies connues depuis de nombreuses années. En effet, l'opération contractuelle du cloud computing n' est pas nouvelle et s'inscrit dans la continuité de la catégorie générique des contrats télématiques et précisément des contrats de traitement à distance. Avant de rentrer dans la technicité de ces figures contractuelles, un travail de définition de celles-ci est effectué ci-après.

***39. Les contrats télématiques.*** Les contrats télématiques correspondent à une catégorie générique de contrats regroupant les contrats qui encadrent un service recourant à la « téléinformatique ». Le terme « télématique » correspond à « l'ensemble des services offerts à l'aide de techniques téléinformatiques »[140]. La téléinformatique se rapporte à « l'ensemble des techniques mettant en œuvre à la fois l'informatique[141] et les télécommunications[142] »[143]. Le contrat télématique professionnel a été défini par certains auteurs comme : « l'ensemble des structures contractuelles ou associatives, qui peuvent être mises en place aux différents stades de la mise sur pied ou de la réalisation d'opérations portant sur un ou des services télématiques professionnels »[144]. Il existe une grande variété de services télématiques, lesquels peuvent être appréhendés, selon le Professeur Poullet, par trois critères ; « le premier est d'ordre technique : on distinguera services diffusés et services interactifs. La distinction porte essentiellement sur le fait que le service interactif, l'identification par télétransmission de l'utilisateur est nécessaire au déclenchement de l'opération ; le deuxième concerne le type d'utilisation du service : il s'agira de services dits grand public ou ouverts par opposition aux services télématiques professionnels, réservés à une utilisation professionnelle ; le troisième met l'accent sur la fonctionnalité du

[140] Poullet Y., introduction aux aspects juridiques des contrats télématiques professionnels, CRID, juillet 1987 : http://www.crid.be/pdf/public/7265.pdf.

[141] Définition de « l'informatique » : il s'agit de « l'ensemble des techniques, méthodes et outils permettant le traitement de l'information. Sa caractéristique principale est qu'elle permet de traiter un volume considérable de données à une très grande vitesse » : Poullet Y., introduction aux aspects juridiques des contrats télématiques professionnels, CRID, juillet 1987 : http://www.crid.be/pdf/public/7265.pdf.

[142] Définition de « télécommunications » : il s'agit de l'ensemble des procédures de transmission d'information à distance quelqu'en soit le support (ondes hertziennes, lignes techniques, cables, fibres optiques, etc..) : Poullet Y., introduction aux aspects juridiques des contrats télématiques professionnels, CRID, juillet 1987 : http://www.crid.be/pdf/public/7265.pdf.

[143] Ibid.

[144] Ibid.

service : la gestion, la communication ou la documentation »[145]. Le dénominateur commun de ces contrats est donc la « téléinformatique » qui correspond à l'informatique faisant appel à des moyens de transmission à distance et le cloud computing en fait naturellement partie. Les contrats télématiques sont des contrats-cadres qui ont pour objet d'encadrer l'exécution des prestations de services recourant à la téléinformatique[146].

***40.*** Cette catégorie générique des « contrats télématiques » intègre d'autres catégories de contrats et parmi elles, les « contrats de prestation téléinformatique » dont l'objet est de fournir des prestations de services à contenu « téléinformatique » exécuté en « ligne ». L'objet de ce contrat est la délivrance, par le détenteur du système, de diverses prestations réalisées en ligne[147]. Ces contrats de prestations téléinformatiques constituent une catégorie de contrats dans laquelle figure une « sous-catégorie » de contrats, « les contrats de fourniture d'énergie informatique » qui contient une autre sous-catégorie de contrats « les contrats de traitement à distance » s'illustrant par deux autres catégories de contrats, « le contrat d'infogérance » et « le contrat SaaS (software as a service) [148] ». Aux fin de compréhension de cette déclinaison, il est annexé à la présente étude un schéma résumant la déclinaison des contrats télématique[149]. En l'espèce, le contrat de cloud computing emprunte à ces différents contrats et en particulier au contrat d'infogérance et au contrat SaaS[150].

***41. Le contrat d'infogérance.*** Lorsqu'une entreprise confie à un prestataire la gestion d'une prestation de services, ce processus correspond à l' « externalisation » ou « outsourcing » . Lorsque l'externalisation est appliquée aux prestations informatiques, on parle "d'infogérance", ou "facilities management". Alors, le contrat d'infogérance « consiste, pour une entreprise à confier à un prestataire extérieur le soin d'héberger, gérer et maintenir l'application informatique permettant d'assurer tout ou partie des traitements de données dont elle a besoin ». Ce contrat est défini comme « le résultat de l'intégration d'un ensemble de services élémentaires, visant à confier à un prestataire informatique tout ou partie du système d'information du client dans le cadre d'un contrat pluriannuel à base forfaitaire avec un niveau

---

[145] Ibid.

[146] Concernant la détermination des contrats télématiques professionnels :Poullet Y., introduction aux aspects juridiques des contrats télématiques professionnels, CRID, juillet 1987 : « la télématique c'est-à-dire les structures mises en place pour la fourniture de service télématiques professionnels » (..) Par contrat télématique professionnel, nous entendons au sens du présent rapport, l'ensemble des structures contractuelles ou associatives, qui peuvent être mises en place aux différents stades de la mise sur pied ou de la réalisation d'opérations portant sur un ou des services télématiques professionnels » : http://www.crid.be/pdf/public/7265.pdf.

[147] Dans ce cas, il s'agit de contrats de prestations téléinformatiques.

[148] Initialement le contrat ASP « Application service provider » lequel est un contrat de prestation de service proposant dans le cadre d'un abonnement, l'utilisation à distance de logiciels et de services informatiques associés.

[149] V. Annexe 2 de la présente étude.

[150] V. *infra* n° 42, contrat SaaS.

de service d'une durée définie »[151]. En d'autres termes, le contrat d'infogérance est un contrat de prestation de services dont l'objet est de confier à un prestataire informatique la gestion et l'exploitation du système informatique (parc informatique, réseaux, maintenance applicative) d'une entité[152]. Concernant le contenu du contrat, il est nécessaire de prévoir des dispositions tenant à l'exécution de la prestation informatique. En particulier, la doctrine précise « pour que l'externalisation s'opère dans de bonnes conditions, et que la continuité de l'exploitation soit assurée, on précisera dans le contrat quels sont les matériels et logiciels qu'il faudra faire passer sous le contrôle du prestataire, comment les données existantes seront transférées et comment les informations produites quotidiennement seront communiquées (…) à la réversibilité de l'application, c'est-à-dire à la possibilité pour l'entreprise cliente de rapatrier celle-ci dans les meilleures conditions (…) Cela implique de préciser dans le détail quels sont les matériels et logiciels qui seront compris dans l'opération de réversion, comment les données seront récupérées»[153]. Le contrat d'infogérance est par sa nature un contrat complexe, lequel est qualifié par la doctrine de « louage d'ouvrage » pour la raison qu'il a pour objet la prise en charge, par le prestataire de la gestion intégrale ou partielle du système informatique du client[154]. Pour arriver à cette qualification, il est important d'identifier la prestation caractéristique dans l'opération voulue et les obligations respectives incombant à chacune des parties au contrat. Ensuite, le contrat de cloud computing emprunte également au contrat SaaS (initialement « ASP » Application Service Provider).

***42. Le contrat ASP (Application Service Provider) ou Saas (Software as a Service).*** Le contrat ASP ou Saas a pour objet d'encadrer la mise à disposition de services informatiques matérialisés par un logiciel, lequel est hébergé dans les serveurs d'un prestataire informatique et utilisé en même temps par plusieurs clients[155]. À la différence du contrat ASP, il est possible de bénéficier d'une personnalisation des applications dans le cadre du contrat SaaS. La spécificité, ici, est que la personnalisation des applications s'opère à distance. Dans un contrat de SaaS, le prestataire permet au client, dans le cadre d'une prestation de fourniture, d'utiliser des logiciels qui sont délocalisés chez le prestataire. La prestation caractéristique du contrat SaaS réside dans le droit d'utiliser le logiciel qui est hébergé dans les serveurs du prestataire. Par la suite, le contrat de SaaS s'est développé et a donné lieu à une multitude de prestations à distance regroupées sous l'expression de « cloud computing ». Dans le cadre d'un contrat de SaaS, le prestataire de

[151] Définition du contrat d'infogérance par l'AFNOR (Association française de normalisation), Norme XP Z67-801-1.

[152] Concernant les spécificités du contrat d'infogérance : Bitan H., Droit et expertise des contrats informatiques : Contrats de communications électroniques - Vision expertale de la protection des données, édition Lamy Axe droit, juin 2019.

[153] Huet J., Contrats informatiques – contenu et typologie, fascicule 322, JurisClasseur Commercial, 20 mars 2013.

[154] Gaudrat Ph. et Sardain F., Traité de droit civil du numérique, Tome 2 Droit des obligations, édition Larcier 2015.

[155] Ibid.

service met à distance et à la disposition de clients un service de nature informatique qui est géré par un programme hébergé dans un serveur identifié et localisé du prestataire. Alors que dans le cloud computing, la localisation du stockage des données est très souvent inconnue pour le client[156].

Qu'il s'agisse du contrat d'infogérance ou du contrat ASP ou SaaS, ils appartiennent à la catégorie des contrats de prestations informatiques qui ont pour objet de « louer, vendre et/ou délivrer une prestation de services informatique (matériel ou logiciel) »[157]. Précisément, il s'agit de « la convention par laquelle une personne ou une société s'oblige contre une rémunération à exécuter pour une autre personne ou une société, un travail relevant du milieu de l'informatique, sans agir en son nom et de façon indépendante » [158]. Les contrats informatiques sont soumis au droit commun des contrats [159] dont les règles sont prévues aux articles 1101 à 1231-7 du code civil) et au droit spécial en fonction de l'objet du contrat et de la nature de la prestation [160].

**3) Les spécificités du contrat de cloud computing**

***43. Des prestations de services diffuses.*** Dans le cadre d'un service de cloud computing « les serveurs (voire les processeurs) sont géographiquement dispersés en de multiples lieux, sur de multiples machines, appartenant à de multiples personnes ou prestataires, lesquels ne sont pas nécessairement connus du client »[161]. Cette différence est fondamentale en matière de protection des données. Ce constat rend difficiles l'application et le respect effectif de la réglementation protectrice des données en vigueur. Par la technologie du cloud computing, les données sont sauvegardées dans des serveurs distants et accessibles seulement par internet.

***44. Les documents contractuels avec une personne physique.*** Dans le cadre d'une relation entre un Prestataire de services de cloud computing et une personne physique, celle-ci se formalise par plusieurs documents contractuels. Ainsi, les « conditions d'utilisation » des services cloud est le document qui va régir la relation contractuelle entre un prestataire de services cloud et l'utilisateur, personne physique. Ces conditions d'utilisation constituent un contrat d'adhésion au sens de l'article 1110 du Code civil[162] dans la mesure où les dispositions ne sont ni

[156] Concernant les spécificités du contrat Saas : Bitan H., Droit et expertise des contrats informatiques : Contrats de communications électroniques - Vision expertale de la protection des données, édition Lamy Axe droit, juin 2019.

[157] Définition de contrat de prestation informatique : https://www.captaincontrat.com/contrats-commerciaux-cgv/contrats-commerciaux/contrat-de-prestation-informatique.

[158] Ibid.

[159] Huet J., Contrats informatiques – Contenu et typologie, Fascicule 322, JurisClasseur Commercial, 20 mars 2013.

[160] Ibid.

[161] Gaudrat Ph. et Sardain F., Traité de droit civil du numérique, page 296, paragraphe 578, *op. cit.*, édition Larcier 2015. V. également, Poidevin B., « le contenu du contrat de cloud computing », RLDI 2013/98, p.104.

[162] Définition du contrat d'adhésion : 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 ».

négociables ni modifiables. Les conditions s'imposent d'un « bloc » à l'utilisateur, personne physique. Pour être en conformité avec le RGPD, les conditions d'utilisation du service cloud prévoient l'exigence de recueillir le consentement de l'utilisateur (personne physique). En pratique, il apparaît que ce consentement est donné de manière « tacite » par l'utilisateur. La jouissance des services de cloud computing est conditionnée à l'acceptation des conditions d'utilisation des services[163]. Parfois, le consentement est considéré comme donné par le simple fait que l'utilisateur utilise le service cloud ou par un simple « clic » engendrant l'application des conditions d'utilisation du service cloud [164]. En sus de ce document contractuel, le prestataire de service de cloud computing intègre les règles relatives à la protection des données à caractère personnel (conformément aux prescriptions du RGPD) dans un document nommé « les règles de confidentialité » ou « la politique de confidentialité » qui constitue un document contractuel. Ce document vient préciser comment le prestataire de services cloud traite et protège les données à caractère personnel (communication d'un certain nombre d'informations tel que les types de données collectées, le but de la collecte des données). Ce document oriente, également, l'utilisateur afin qu'il puisse être en mesure de protéger et gérer ses données, les exporter et les supprimer. Par principe, la conclusion du contrat de cloud computing entre une personne physique qualifiée ici de « consommateur »[165] et le prestataire de services cloud est réalisée de manière électronique. En ce sens, ce contrat de cloud computing est considéré comme étant un contrat électronique dès lors que les conditions légales prévues aux articles 1125 à 1127-4 du code civil et à l'article L.213-1 du code de la consommation sont remplies. Concernant le cadre de ces contrats, l'article 1127-1 du code civil précise les mentions devant figurer dans une offre proposée par voie électronique et l'article 1127-2 du code civil les conditions de validité d'un contrat électronique.

***45. Les documents contractuels avec une personne morale*** : Le contrat de cloud computing conclu entre un prestataire de services cloud et une personne morale est un contrat-cadre informatique. Au sein de ce contrat figure des annexes contractuelles dont les intitulés sont à l'origine en anglais puis traduits en français. L'opération contractuelle est encadrée par « *The Master Service Agreement (MSA) »*[166], soit en français le contrat-cadre de services qui a pour objet de fixer le

[163] À titre d'exemple, il est précisé dans des conditions d'utilisation de Google que « l'utilisation de nos Services implique votre acceptation des présentes Conditions d'Utilisation [..] Vous devez respecter les règles applicables aux Services que vous utilisez » : Les conditions d'utilisation du service cloud de Google : https://policies.Google.com/terms.

[164] Par exemple, dans les conditions d'utilisation des services i-cloud d'Apple, il est expressément mentionné que « de cliquer sur « accepter » engendre l'application des présentes conditions à l'utilisateur dès lors qu'il y a eu un accès ou une utilisation du service i-cloud » : Les conditions d'utilisation des services i-cloud d'Apple : https://www.apple.com/legal/internet-services/icloud/fr/terms.html.

[165] Définition « consommateur », article liminaire du code de la consommation : « Est un consommateur une personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité professionnelle ».

[166] Dalloz référence Contrats du numérique, Lexique anglo-français de termes de l'informatique et de l'internet – 2021/22.

cadre des relations contractuelles et en précise les modalités d'exécution, les conditions de prestations de services à venir. Cet accord-cadre est accompagné de diverses annexes telles que : « *The Cloud particulars terms* », il s'agit d'une annexe relative aux conditions particulières qui ont été spécialement convenues entre les parties au contrat ; ensuite, « *The Statement of work* » (SOW), il s'agit du cahier des charges lequel a pour objet de décrire précisément les besoins attendus par le client et auxquels le prestataire doit répondre[167] ; « The Service Level Agreement » (SLA) traduit en français par « la convention de services »[168], il s'agit d'un accord du niveau de service attendu qui a pour objet « de traiter les questions relatives au taux de disponibilité de l'application, à la rapidité des traitements envisagés (envoi et restauration des données), à la fréquence des sauvegardes »[169]. Le « SLA » est « un document dans lequel le prestataire formalise la qualité du service et précise notamment les modalités, la performance du service (temps de réponse, temps de transmission des données…), la disponibilité des applications (horaires d'ouverture et fermeture, période d'indisponibilités…) »[170]. En cas de manquement aux obligations conventionnelles relatives à la qualité du service de cloud computing, c'est ce document qui peut prévoir des pénalités. Le SLA est un document technique qui vise à mesurer la qualité du service rendu, et ce au travers d'indicateurs clés appelés « Key Performance Indicators (KPI) ». Pour permettre aux parties de négocier le SLA, il faut s'interroger en amont sur l'assiette des services concernés par le SLA. Autrement dit, il convient de vérifier le niveau de couverture des services et leur degré de qualité au travers des KPI. Les deux critères utilisés, pour mesurer la qualité des services couverts par le SLA, sont « la disponibilité » et « la continuité » du service appréhendées selon une période. En cas de manquements aux obligations du SLA par le prestataire, des sanctions peuvent être prévues, telles que « des rabais mensuels (en pourcentage) sur les montants dus, en proportion de la performance réalisée par le prestataire dans le mois précédent, des réductions spécifiques, préagréées, en cas de non-atteinte des seuils de performance et la résiliation du contrat en cas de violation chronique des SLA »[171]. Ensuite, figure « The Ad-hoc order form »

[167] Le Tourneau Ph., Contrats du numérique, informatiques et électroniques, Dalloz, Dalloz, 12e édition, 2022-2023, p.462 n°342-15.

[168] Guide, Contractualisation des services cloud, les enjeux juridiques, Staub & Associes : https://www.eurocloud.fr/doc/guide-contractuel-cloud.pdf.

[169] Flipo O. et Forest D., « Contrats : la disponibilité dans les contrats SaaS », Expertises 2012, p.146.

[170] Définition du SLA : Warusfel B. (sous la direction de Vivant M.), Le Lamy droit du numérique 2018, Expert, Partie 3 - Numérique et contrats, division 3 - Les principaux contrats du numérique et leurs spécificités, chapitre 6 - Les contrats d'informatique dématérialisée (cloud computing), p.492 n°708, mis à jour 22 avril 2022. Egalement, cet ouvrage précise les documents de référence pour rédiger cette convention de niveau de services : Document de l'Autorité nationale de la sécurité des systèmes d'information (ANSSI) « Maîtriser les risques d'infogérance » (et plus particulièrement son chapitre 4 : le plan d'assurance sécurité) ; également, document rédigé au niveau européen par le C-SIG « Cloud Service Level Agreement Standardisation Guidelines », 24 juin 2014.

[171] Guidelines de l'Information Technology Association of America (ITAAA) accessibles sur le site www.itaa.org. V. également, Warusfel B. (sous la direction de Vivant M.), Le Lamy droit du numérique 2018, Expert, Partie 3 - Numérique et contrats, division 3 - Les principaux contrats du numérique et leurs spécificités, chapitre 6 - Les contrats d'informatique dématérialisée (cloud computing), p.493 n° 708, mis à jour 22 avril 2022.

soit en français « le formulaire d'acceptation » lequel permet aux clients de donner son consentement à la réalisation de prestations de services spécifiques et l'annexe « The Acceptable Use Policy » (AUP), traduit par *l'acceptation de la politique d'utilisation,* qui est un document contractuel relatif aux conditions d'utilisation du service cloud. Le contrat de cloud computing conclu avec une personne morale est un contrat qui intègre ces différentes annexes contractuelles. Après avoir observé les documents contractuels, il est envisagé, à présent, la diversité des infrastructures de cloud computing.

***46. La variété des infrastructures de cloud computing.*** Aujourd'hui, on en dénombre quatre principaux types de Cloud : le cloud privé, le cloud public, le cloud hybride, le cloud communautaire [172]. Le « cloud privé » ou le « cloud dédié » correspond à une infrastructure consacrée entièrement au client, ce qui signifie qu'il dispose de serveurs privatifs qui vont gérer l'ensemble de ses données. Ce type de cloud peut être administré soit en interne, c'est-à-dire sur le site du client, soit à l'extérieur de l'entreprise par un prestataire spécialisée. Ce type d'administration de cloud s'apparente à une infrastructure locale[173]. Le « cloud public » ou le « cloud mutualisé » correspond à une infrastructure dont les ressources informatiques des serveurs sont partagées par l'intermédiaire d'internet. Le prestataire de services cloud demeure propriétaire de l'infrastructure physique et gère la maintenance. La facturation des services de cloud public a pour base l'utilisation des données dans le serveur. Ainsi, plus le client héberge, utilise ou télécharge d'informations dans le serveur et plus il sera amené à payer. Le cloud public permet, donc, de stocker les données sur plusieurs serveurs accessibles par des utilisateurs déterminés [174]. Puis, le « cloud hybride » correspond à un système mixte d'infrastructure cloud, c'est-à-dire qu'il s'agit d'avoir pour le client une partie de son infrastructure informatique en cloud privé et une autre partie en cloud public. Les deux infrastructures cloud gardent leur indépendance de fonctionnement l'une envers l'autre[175]. Enfin

[172] Thèse de Medhioub H., Architectures et mécanismes de fédération dans les environnements Cloud Computing et Cloud Networking, Telecom Sudparis et l'Université Pierre et Marie Curie, 28 avril 2015.

[173] Définition du cloud privé : « Dans un Cloud Privé, l'utilisateur des ressources Cloud Computing contrôle, voire possède, l'infrastructure d'hébergement. Les ressources disponibles ne sont pas desti- nées au grand public, mais pour une utilisation privée. Dans ce type de déploiement, l'infrastructure est gérée avec des solutions (Open Source ou propriétaire) de type Cloud pour offrir les ressources et services par le biais d'interface Cloud » Thèse de Medhioub H., Architectures et mécanismes de fédération dans les environnements Cloud Computing et Cloud Networking, Telecom Sudparis et l'Université Pierre et Marie Curie, 28 Avril 2015. V. également, article concernant l'infrastructure cloud : http://www.computerland.fr/difference-cloud-prive-public/.

[174] Définition du cloud public : « Dans un Cloud Public, le fournisseur gère l'infrastructure et offre ses services aux utilisateurs Cloud grand public d'une façon complètement ouverte. Les ressources informatiques sont partagées entre les utilisateurs. Ces derniers n'ont aucun contrôle ou visibilité sur l'infrastructure qui est gérée par un tiers (le fournisseur de Cloud) » : thèse de Medhioub H., Architectures et mécanismes de fédération dans les environnements Cloud Computing et Cloud Networking, Telecom Sudparis et l'Université Pierre et Marie Curie, 28 Avril 2015. Également, V. également, article concernant l'infrastructure cloud : http://www.computerland.fr/difference-cloud-prive-public/.

[175] Définition du cloud hybride : « Dans un Cloud Hybride, les ressources peuvent être allouées à partir d'un Cloud Privé et d'un Cloud Public. C'est un environnement qui combine les deux modèles Public et Privé. Comme utilisation de ce type de Cloud

le « cloud communautaire », il s'agit d'une infrastructure cloud partagée « par plusieurs membres ou organisations (des PME par exemple), réunis au sein d'une communauté et partageant des préoccupations spécifiques communes : par exemple la mission, les exigences de sécurité, des politiques et des considérations de conformité. Elle peut être gérée par les organisations ou par un tiers et peut exister sur site ou hors site »[176]. Dans le cadre de l'étude des contrats cloud pour apprécier le niveau de protection des données, il est envisagé de prendre en considération les spécificités attachées au type d'infrastructure choisi par le client. Si les infrastructures nous renseignent sur le cadre dans lequel le cloud sera amené à se développer, les différentes prestations pouvant être proposées en matière de cloud constituent le contenu qui sera retranscrit en matière de droits et d'obligations dans le contrat de cloud computing. En annexe est présenté, un schéma synthétique des types d'infrastructures cloud privé et public [177].

***47. La diversité des prestations de services de cloud computing.*** Le cloud computing recouvre une variété de solutions de stockage de données classées en trois catégories de services : IaaS (Infrastructure As A Service, traduit par Infrastructure en tant que Service), PaaS (Platform As A Service, traduit par Plateforme en tant que Service), Saas (Software As A Service, traduit par Logiciel en tant que Service)[178] lesquels font l'objet d'un contrat de cloud computing spécifique.

***48.*** Dans le cadre de la prestation IaaS, le prestataire de service va octroyer à un client l'accès à un parc informatique virtualisé et l'hébergement classiques des données. En d'autres termes, le client bénéficie d'un accès à un parc informatique et pourra installer son propre système d'exploitation et ses propres applications. En l'espèce, le client achète une certaine puissance

---

Hybride, il est possible de stocker et gérer les données confidentielles dans l'environnement privé et celles qui sont moins confidentielles dans un Cloud Public. Une autre utilisation est d'avoir recours aux ressources Cloud publiques d'une façon ponctuelle, lors des pics d'activité » : Thèse de Medhioub H., Architectures et mécanismes de fédération dans les environnements Cloud Computing et Cloud Networking, Telecom Sudparis et l'Université Pierre et Marie Curie, 28 Avril 2015. Également, V. également, article concernant l'infrastructure cloud : http://www.computerland.fr/difference-cloud-prive-public/.

[176] Définition du cloud communautaire : « Dans un Cloud Communautaire, l'infrastructure de Cloud est provisionnée à l'usage exclusif d'une communauté d'utilisateurs, par exemple les organismes gouvernemen- taux. L'infrastructure peut être détenue, gérée et exploitée par un ou plusieurs des organismes de la communauté, un tiers, ou une combinaison d'entre eux » : thèse de Medhioub H., Architectures et mécanismes de fédération dans les environnements Cloud Computing et Cloud Networking, Telecom Sudparis et l'Université Pierre et Marie Curie, 28 Avril 2015. V. également, article concernant l'infrastructure cloud : http://www.computerland.fr/difference-cloud-prive-public/.

[177] V. annexe 3 de la présente étude, schéma, La distinction des infrastructures cloud public, privé, hybride.

[178] Contrats du numérique, informatiques et électroniques, Le Tourneau Ph., Dalloz, Dalloz, 12e édition, 2022-2023, p.461 n°342-14. Egalement, V. Warusfel B. (sous la direction de Vivant M.), Le Lamy droit du numérique 2018, Expert, Partie 3 - Numérique et contrats, division 3 - Les principaux contrats du numérique et leurs spécificités, chapitre 6 - Les contrats d'informatique dématérialisée (cloud computing), p.493 n° 708, mis à jour 22 avril 2022: Il existe trois types de prestations de services, pouvant être proposées en cloud computing, identifiées sous les appellations suivantes : « IaaS (Infrastructure as a service) », « PaaS (Platform as a service) », « Saas (Software as a service) ». V. également, Syntec numerique, Les contrats Cloud : des contrats clés en main, 15 octobre 2015, disponible sur http://www.afdit.fr/media/pdf/15%20oct%202015/M%20Coulaud%20Contrats%20cloud.pdf.

informatique, laquelle est décomptée en nombre de machines virtuelles et ne se préoccupe pas de l'achat d'une infrastructure informatique physique[179].

***49.*** Dans le cadre de la prestation de service PaaS, le client délègue un peu plus de responsabilités au prestataire. Il peut, ainsi, décider de mettre, sous sa responsabilité, le système d'exploitation et les outils d'infrastructures. De manière synthétique dans le cadre d'une prestation de services PaaS, le client loue l'exploitation des serveurs ainsi que les outils qui sont sous la responsabilité du prestataire[180].

***50.*** Enfin, dans le cadre de la prestation de services SaaS : Il s'agit d'une prestation offerte par le prestataire au client « clé en main ». Le client ne se préoccupe pas des dysfonctionnements du logiciel, lesquels sont pris en charge et résolus par le prestataire.[181]

***51.*** La sélection d'un type de services cloud produit des droits et des obligations pour les parties au contrat de cloud computing. Le contrat cloud est, alors, spécifique en fonction des parties au contrat, du type d'infrastructure et de la prestation de services choisis par le client. En annexe de la présente étude figure un schéma présentant la distinction IaaS, PaaS, SaaS (annexe 1).

***52.*** Après avoir introduit le sujet par des éléments de définitions et de contexte, il convient d'exposer l'approche et la méthodologie retenues.

---

[179] Définition des prestations de IaaS « Les services Cloud Computing de type IaaS correspondent à des ressources infrastruc- tures offertes à la demande. Ces ressources sont des ressources de calculs, de stockage ou de réseau et peuvent être soit virtuelles, soit physiques. Le fournisseur a la gestion des couches Calcul, Stockage, Réseau et Virtulisation. L'utilisateur des ressources IaaS est responsable de la gestion de toutes les couches à partir et au-dessus du système d'exploitation. L'utilisateur n'a ni le contrôle, ni la gestion, ni la visibilité de l'infrastructure sous-jacente » : Thèse de Medhioub H., Architectures et mécanismes de fédération dans les environnements Cloud Computing et Cloud Networking, Telecom Sudparis et l'Université Pierre et Marie Curie, 28 Avril 2015.

[180] Définition des prestations de PaaS : « Les services Cloud Computing de type PaaS correspondent principalement à des environnements de développement offerts à la demande. L'utilisateur n'a plus en charge que les couches de données et d'applications. Pour ce faire, il y a utilisation des librairies, langages et outils offerts par le fournisseur pour structurer ses données et développer ses applications. Une fois développé, le fournisseur doit déployer et maintenir le bon fonctionnement de l'application et cela en gérant toutes les couches basses allant de l'infrastructure jusqu'aux environnements d'exécution » : : Thèse de Medhioub H., Architectures et mécanismes de fédération dans les environnements Cloud Computing et Cloud Networking, Telecom Sudparis et l'Université Pierre et Marie Curie, 28 Avril 2015.

[181] Définition des prestations de SaaS : « Les services Cloud Computing de type SaaS correspondent tout simplement à des applications prêtes à l'utilisation offertes à la demande. L'utilisateur n'a qu'à utiliser le service Cloud Computing offert. Il n'a rien à gérer et c'est le fournisseur qui a toute la responsabilité de maintenir le service en gérant toutes les couches (..) » : Thèse de Medhioub H., Architectures et mécanismes de fédération dans les environnements Cloud Computing et Cloud Networking, Telecom Sudparis et l'Université Pierre et Marie Curie, 28 Avril 2015. Illustration : La location du logiciel de Microsoft office sur une base mensuelle, les logiciels professionnels tels que photoshop, Hootsuite, Salesforce, ou encore les logiciels de courriel (hotmail, Gmail…) ou les espaces de stockage en ligne (icloud, Google drive…) sont des prestations de services Saas. D'un point du vue technique, l'avantage principal de cette offre « clé en main » permet de décharger le client de la résolution des dysfonctionnements lesquels incombent au prestataire.

## Section 2 : Les moyens du renforcement de la protection des données dans les contrats de cloud computing

***53.*** Le caractère protéiforme du Cloud computing, son intangibilité et la difficulté à le saisir à l'aide des schémas traditionnels, notamment en matière de protection des données, obligent à un changement de paradigme pour trouver les solutions juridiques adaptées assurant de *lege ferenda* la protection des données dans le cadre du cloud computing[182]. La problématique est la suivante ; comment renforcer la protection des données dans les contrats de cloud computing ?

***54.*** La réflexion est menée à partir du triptyque suivant : la protection technologique, la protection légale et la protection contractuelle. Tout d'abord, il apparaît que la protection des données passe en premier lieu par une protection technologique. C'est pour cette raison qu'il est opportun d'envisager, cette protection technologique avant d'étudier la protection des données par la loi et le contrat. La raison de cette approche se fonde principalement sur le constat que la protection technologique est un prérequis à l'utilisation d'un service technologique, le cloud computing.

***55.*** **Plan.** Il est envisagé d'étudier la manière dont le droit réglemente ces mesures techniques pour qu'elles soient effectives (I) sur le plan de la protection des données. En définitive, il apparaît que la protection technologique à elle seule est insuffisante pour permettre une protection optimale des données dans l'exécution d'un contrat de cloud computing, il est nécessaire de la renforcer par la loi et le contrat. À cette fin, l'étude est fondée sur une analyse des droits et l'élaboration d'un cadre protecteur (II).

### I. L'étude de la protection des données par la technologie

***56.*** ***Le régime des mesures techniques*** : Les données sont hébergées (stockées) dans le nuage (cloud computing) et sont accessibles par une connexion internet. Afin de sécuriser les données hébergées dans le nuage, l'infrastructure cloud (des serveurs distants et reliés par une connexion internet) doit faire l'objet de mesures techniques. Ces mesures techniques se sont développées ces dernières années en raison de l'essor de l'utilisation des outils informatiques et digitaux. La question est de savoir si ces mesures sont appréhendées par le droit. Le Code de la propriété intellectuelle définit les mesures techniques de protection (MTP). Ces mesures visent : « à empêcher ou à limiter les utilisations non autorisées par les titulaires d'un droit d'auteur ou d'un

[182] Sur ce point, Brunaux G., a considéré qu' « en réalité, c'est le caractère protéiforme du cloud computing qui pose problème » Brunaux G., Cloud computing, protection des données : et si la solution résidait dans le droit des contrats spéciaux ?, D. 2013, p. 1158.

droit voisin du droit d'auteur d'une œuvre ». Il est indiqué que ces mesures reposent sur : « toute technologie, dispositif » utilisant « l'application d'un code d'accès, d'un procédé de protection tel que le cryptage, le brouillage ou toute autre transformation de l'objet de la protection ou d'un mécanisme de contrôle de la copie qui atteint cet objectif de protection »[183]. Ces mesures techniques sont, ici, qualifiées de « cryptage », de « brouillage », ou de « mécanisme de contrôle » et ne portent que sur l'objet de la protection en l'occurrence. En matière de cloud computing, l'objet à protéger est la « donnée ».

***57. L'analyse dichotomique des mesures techniques de protection des données.*** Avant d'envisager l'étude de la protection légale et contractuelle des données dans les contrats de cloud computing, la sécurisation technologique est un prérequis à l'utilisation d'un service de cloud computing. Le cloud computing étant une technologie, celui-ci doit être conçu avec un protocole de sécurité technique avant même de pouvoir faire l'objet d'une formalisation contractuelle. Les mesures techniques font l'objet d'une présentation dichotomique entre, d'un côté, celles visant la sécurité de l'infrastructure cloud et de l'autre, celles se rapportant à la sécurité des données. Il convient d'envisager le cadre légal de ces mesures techniques [184]. Il apparaît que des règles spécifiques s'appliquent à chacune de ces mesures. Ensuite, il est envisagé de les analyser afin de les appliquer à la protection des données dans les contrats de cloud computing. Il est très vite constaté que ces mesures techniques ne suffisent pas à elles seules pour protéger les données dans le cloud et l'intervention d'un « droit dur » s'avère nécessaire. Par « droit dur », on entend un droit contraignant, au sens de la conception classique romaine de « lex perfecta », c'est-à-dire, une loi prévoyant des sanctions pour la violation des règles [185].

---

[183] Définition des MTP, article L. 331-5 du code de la propriété intellectuelle : « (..) destinées à empêcher ou à limiter les utilisations non autorisées par les titulaires d'un droit d'auteur ou d'un droit voisin du droit d'auteur d'une œuvre, autre qu'un logiciel, d'une interprétation, d'un phonogramme, d'un vidéogramme ou d'un programme sont protégées dans les conditions prévues au présent titre on entend par mesure technique au sens du premier alinéa toute technologie, dispositif, composant qui, dans le cadre normal de son fonctionnement, accomplit la fonction prévue par cet alinéa. Ces mesures techniques sont réputées efficaces lorsqu'une utilisation visée au même alinéa est contrôlée par les titulaires de droits grâce à l'application d'un code d'accès, d'un procédé de protection tel que le cryptage, le brouillage ou toute autre transformation de l'objet de la protection ou d'un mécanisme de contrôle de la copie qui atteint cet objectif de protection ».

[184] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. Dir. Parl. et Cons. CE nº 2002/21/CE, 7 mars 2002, JOCE 24 avr. 2002, nº L 108 concernant le cadre réglementaire commun pour les réseaux et services de communications électroniques (directive "cadre"). Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique : L. nº 2004-575, 21 juin 2004, JO 22 juin. Loi du 15 novembre 2001 relative à la sécurité quotidienne : L. nº 2001-1062, 15 nov. 2001, JO 16 nov. Articles 230-1 à 230-5 du Code de procédure pénale : dispositions permettant aux autorités judiciaires d'obtenir « la mise au clair des données chiffrées nécessaires à la manifestation de la vérité », c'est-à-dire d'informations inintelligibles ou cryptées. Également, le référentiel ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) du 30 juillet 2014 sur les prestataires de services sécurisés d'informatique en nuage, la norme ISO/IEC 27018 constituant les bonnes pratiques pour la protection des données personnelles dans les services de Cloud, la norme ISO/IEC 27017 en matière de sécurité du Cloud, la norme ISO 19086 sur la notion de niveau de service.

[185] Kornbeck J., Droit dur ou mou ? L'Union européenne et la promotion des APS, Jurisport 2021, n°216, p.39 ; V. Deroussin D., Soft law : éléments historiques in Deumier P., Sorel J.-M. (dir.) Regards croisés sur la soft law en droit interne, européen et international, LGDJ, 2018, p. 55-76, v. p. 63.

***58.* Plan.** Il est envisagé, tout d'abord, d'étudier les différentes mesures techniques de sécurité des données numériques dans le cloud computing. Il existe plusieurs mesures techniques permettant de sécuriser, d'une part, l'infrastructure cloud et, d'autre part, la donnée cloud (A). À la suite de cette identification, il sera envisagé d'étudier la place qu'occupent dans le contrat cloud ces mesures techniques pour assurer la protection des données (B).

## A) La détermination des mesures techniques

***59.* Plan.** Pour assurer la protection des données dans le cloud computing, il est envisagé d'étudier les mesures techniques relatives à la sécurisation, d'une part, de l'infrastructure cloud (1) et d'autre part, des données stockées dans le cloud (2).

### 1) La protection des données par la sécurisation technologique de l'infrastructure cloud

***60.*** Au fil des années, les mesures techniques relatives à la sécurisation de l'infrastructure cloud se sont développées afin d'offrir aux clients un service cloud sécurisé contre notamment une intrusion de tiers dans le réseau. Parmi ces mesures techniques de sécurisation de l'infrastructure cloud, il est fait appel aux éléments de sécurité issus du protocole TCP/IP (Transfert Control Protocol/internet), au firewall, au mécanisme du « Public Key Infrastructure » et au suivi des contrôles d'accès. Ces processus se sont développés spécifiquement pour accroître la sécurité liée à l'interconnexion de réseaux virtuels de type IP (internet Protocol) à l'internet. L'infrastructure cloud computing fonctionne en réseau avec des serveurs distants et reliés par une connexion internet. Il est question, ici, d'identifier chacune de ces mesures techniques afin d'être en mesure de les appréhender et de les intégrer dans le contrat de cloud computing.

***61. Les mesures de sécurité issues du protocole TCP/IP (Transfert Control Protocol/internet).*** Les mesures techniques de sécurisation de l'infrastructure cloud issues du protocole TCP/IP correspondent à l'utilisation des algorithmes qui vont garantir que « les données envoyées depuis une adresse IP sont identiques à celles qui arrivent à l'adresse IP de destination »[186]. Ainsi, par ce protocole, on garantit l'intégrité de la donnée en transit dans le réseau. Ce type de mesure permet de garantir au titulaire de sa donnée que celle-ci ne sera pas altérée entre l'envoi

[186] Adda H., McDermott W., Aarpi E., Le Lamy droit du numérique (Guide), Partie 6, Titre 2 Comment sécuriser les systèmes et les réseaux ? Chapitre 1 La sécurité « physique », Section 2 La problématique de la sécurité des réseaux, § 2. L'exemple des réseaux sociaux : la cyberdélinquance et le cyberterrorisme, 2931 - Le niveau de sécurité actuellement disponible, mai 2021.

et l'arrivée de celle-ci dans le serveur. Elle figure parmi les mesures techniques permettant de renforcer la protection technologique de l'infrastructure cloud.

***62. Le firewall ou pare-feu informatique.*** La mesure technique de « firewall »[187] a pour objet de se prémunir contre l'intrusion de tiers dans le réseau. Techniquement, la mesure de « firewall » permet de filtrer les entrées dans le réseau de deux manières : « la première utilise l'information au niveau de l'adresse IP pour vérifier chaque paquet IP afin de déterminer s'il est acceptable ou non. La seconde est fondée sur des serveurs logiciels intermédiaires appelés "proxys" qui analysent les données entrantes, en vérifient l'authenticité et déterminent si ces données sont acceptables ou non, puis stockent ou rejettent les données en vue d'une éventuelle analyse des sources »[188]. Le firewall est conçu par des programmes « secure proxy »[189]. Dans cette configuration, c'est la partie infrastructure cloud que l'on sécurise avec « la mise en œuvre d'un équipement spécifique de filtrage ou d'analyse de flux tels que le firewall, les sondes de détection d'intrusions (…)[190]. La mesure technique de "firewall" permet de se prémunir contre des actions de "piraterie informatique" de l'infrastructure cloud.

***63. La PKI (Public Key Infrastructure).*** La PKI est une mesure technique permettant, aussi, de sécuriser l'infrastructure cloud par la mise en place d'un système de "clés". Cette mesure technique sécurise, également, la transmission et la réception des données dans le réseau. Techniquement, la PKI "est un système de gestion des clés publiques qui permet de gérer des listes importantes de clés publiques et d'en assurer la fiabilité, pour des entités généralement dans un réseau"[191]. Une infrastructure PKI permet de fournir quatre types de services que sont la fabrication de bi-clés, la certification de clé publique et publication de certificats, la révocation de certificats, la gestion de la fonction de certification[192]. D'un point de vue technique, "une

---

[187] Pare-feu informatique, définition du Larousse : Équipement situé entre le réseau Internet et le réseau privé d'une entreprise pour accroître la sécurité de ce dernier en filtrant le trafic en provenance ou à destination d'Internet (calque de l'anglais *fire-wall*).

[188] Adda H., McDermott W., Aarpi E., Le Lamy droit du numérique (Guide), Partie 6, Titre 2 Comment sécuriser les systèmes et les réseaux ? Chapitre 1 La sécurité « physique », Section 2 La problématique de la sécurité des réseaux, § 2. L'exemple des réseaux sociaux : la cyberdélinquance et le cyberterrorisme, 2931 - Le niveau de sécurité actuellement disponible, mai 2021.

[189] « Ces programmes doivent être écrits pour chaque application susceptible d'entrer en contact avec l'extérieur. La connexion proxy de l'application client autorisée avec l'application serveur (firewall) est assurée par une passerelle intitulée « socks ». Chaque révision de ces applications nécessitera donc une modification du programme de sécurité. Les communications diffusées et authentifiées entre deux firewalls ou entre un poste nomade et un firewall créent un réseau privé virtuel – Virtual Private Network (VPN) – par-dessus l'internet public » : Le Lamy droit du numérique (Guide), Partie 6, Titre 2 Comment sécuriser les systèmes et les réseaux ? - Chapitre 1 La sécurité « physique », Section 2 La problématique de la sécurité des réseaux, § 2. L'exemple des réseaux sociaux : la cyberdélinquance et le cyberterrorisme, 2931 - Le niveau de sécurité actuellement disponible, mis à jour 04/2020.

[190] Ibid.

[191] Benjada M., PKI (Public Key Infrastructure), qu'est-ce que c'est ? 14 mars 2001 : https://www.securiteinfo.com/cryptographie/pki.shtml.

[192] Ibid.

infrastructure à clé publique utilise des mécanismes de signature et certifie des clés publiques qui permettent de chiffrer et de signer des messages ainsi que des flux de données, afin d'assurer la confidentialité, l'authentification, l'intégrité et la non-répudiation"[193]. Ce mécanisme permet, ainsi, de sécuriser la signature pour l'intégration d'une bi-clé ; il sera, donc, exigé une clé (privée) pour la création de signatures et une clé (publique) pour la vérification de la signature. L'utilisateur par ce mécanisme devra obtenir un certificat numérique pour accéder aux informations et devra donc faire sa demande auprès d'une "autorité d'enregistrement" qui appréciera la demande en fonction des critères définis par "une autorité de certification"[194]. Ce mécanisme intègre la cryptographie à clé publique et certificat numérique et permet de sécuriser les données numériques des intéressés[195]. Cette mesure technique permet, ainsi, d'installer des éléments de sécurité tels que la confidentialité, l'authentification, l'intégrité et la non-répudiation[196]. La mesure technique de PKI est indispensable dans le cadre de la sécurisation de l'infrastructure cloud, mais également la transmission et la réception des données dans le réseau en garantissant, par l'utilisation des "clés", la confidentialité et l'intégrité des données.

***64. Le contrôle d'accès.*** La mesure technique du *contrôle d'accès* permet de sécuriser l'infrastructure cloud. Elle correspond aux différentes solutions techniques permettant de sécuriser et de gérer les accès physiques à un site ou les accès logiques à un système d'information. Il existe deux types de contrôle d'accès que l'on nomme "le contrôle d'accès physique" et "le contrôle d'accès logique"[197]. Au sein des entreprises disposant des serveurs, il est possible de restreindre l'accès aux emplacements physiques uniquement aux personnes autorisées. Concrètement, cela se traduit par la mise à disposition d'un badge uniquement aux personnes autorisées. Ce badge contient les applications de sécurité professionnelle et est très souvent équipé du "Contrôle d'accès logique (LAC) aux réseaux, stations de travail, e-mail ou chiffrement et signature de données, contrôle d'accès physique (PAC) aux bâtiments, bureaux et zones réglementées ainsi qu'à l'identification visuelle du titulaire de la carte"[198]. Les entreprises

[193] Ibid.

[194] Ibid.

[195] Ibid.

[196] Ibid.

[197] Définition contrôle d'accès : « Le contrôle d'accès à un système d'information, consiste à associer des droits d'accès et/ou des ressources à une entité (personne, ordinateur …), permettant ainsi à l'entité d'accéder à la ressource souhaitée, si elle en a les droits. Un contrôle d'accès peut être logique et/ou physique (mot de passe, carte, clé, biométrie, …), et offre la possibilité d'accéder à : des ressources physiques : un bâtiment, un local, ou logiques : un système informatique par exemple : un système d'exploitation ou une application spécifique. Le contrôle d'accès à un système d'information est généralement étudié suivant le protocole AAA (en anglais : Authentication Authorization Accounting) : https://www.techno-science.net/definition/7383.html et V. https://fr.wikipedia.org/wiki/Contrôle_d%27accès.

[198] https://www.techno-science.net/definition/7383.html et V. https://fr.wikipedia.org/wiki/Contrôle_d%27accès et V. https://safenet.gemalto.fr/Solutions/Data_Protection/Authentication/Contrôle_d_accès_logique_et_physique/.

répertorient leurs accès informatiques à partir d'un "Reporting des Droits d'Accès"[199]. Cette mesure technique est donc, nécessaire, et doit être mise en place afin de sécuriser l'infrastructure cloud contre l'intrusion de tiers dans le réseau et éviter ainsi des actions de "piraterie informatique".

**2) La protection des données par la sécurisation technologique de la donnée**

***65.*** Outre la sécurisation de l'infrastructure cloud, il est également fondamental que des mesures techniques soient également appliquées aux données lesquelles peuvent prendre la forme d'un chiffrement des données, mais aussi les sauvegardes. Il est présenté, ci-dessous, les mesures techniques permettant de protéger les données stockées dans le cloud.

***66. Le chiffrement.*** Le chiffrement est la technologie qui permet de convertir des données d'un format lisible à un format codé et dont la lecture ne peut avoir lieu qu'après les avoir déchiffrées[200]. Cette technologie permet de sécuriser les données contre le vol ou la lecture non autorisée. Il existe plusieurs types de chiffrement, à titre d'exemple, nous avons les protocoles TLS[201] et SSL[202]. Le protocole TLS est "un protocole qui assure la confidentialité des échanges entre les applications de communication et les utilisateurs sur internet. Lorsqu'un serveur et un client communiquent, le TLS s'assure qu'aucun tiers ne peut intercepter ni falsifier un message. Le TLS succède au protocole SSL (Secure Sockets Layer). Le TLS est composé de deux sous-protocoles : le TLS Record et le TLS Handshake. Le protocole TLS Record assure la sécurité des connexions avec des méthodes de chiffrement telles que DES (Data Encryption Standard). Il peut également être utilisé sans chiffrement. Le protocole TLS Handshake permet au serveur et au client de s'authentifier et de négocier un algorithme de chiffrement et des clés de chiffrement avant l'échange des données"[203]. Cette protection des données par le chiffrement ne permet pas d'avoir une protection absolue contre toute attaque ou menace de tiers. Lorsque cette technologie a été conçue, il s'est développé en parallèle des logiciels permettant d'intercepter les données et de les déchiffrer. À titre d'exemple, il existe deux méthodes, la clé de chiffrement symétrique ou algorithme à clé secrète et la cryptographie asymétrique. Tout d'abord, la clé de chiffrement symétrique ou algorithme à clé secrète, il s'agit "d'une méthode de décodage unique qui doit être fournie au destinataire avant que le message ne puisse être déchiffré. La clé

[199] Ibid.

[200] Définition, le chiffrement « est le procédé grâce auquel on peut rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement » : https://www.techno-science.net/definition/6143.html.

[201] TLS : Transport Layer Securité; en français "sécurité de la couche de transport ».

[202] SSL : Secure Sockets Layer ; en français « couches de sockets sécurisés ». Le terme « Socket » est utilisé en informatique pour désigner un connecteur réseau ou une interface de connexion.

[203] La distinction entre TLS et SSL : https://www.lemagit.fr/definition/Transport-Layer-Security-TLS.

utilisée pour encoder est la même que celle utilisée pour décoder"[204]. Puis, la cryptographie asymétrique correspond à la méthode qui utilise deux clés différentes (publique et privée) mathématiquement reliées. Concrètement, les clés se composent uniquement de grands nombres qui ont été couplés entre eux, mais ne sont pas identiques, d'où le terme asymétrique. La clé publique peut être partagée avec tout le monde, mais la clé privée doit rester secrète. Les deux peuvent être utilisées pour chiffrer un message, et la clé opposée à celle utilisée à l'origine pour chiffrer ce message est ensuite utilisée pour le décoder »[205]. Par conséquent, le chiffrement certes permet de sécuriser les données, mais cette protection est relative dans la mesure qu'il existe des technologies pour déchiffrer les données.

***67. Les sauvegardes.*** Les sauvegardes font partie des mesures techniques de protection des données et sont intégrées dans les politiques de sécurité intégrées dans le contrat de cloud computing. Le mécanisme de la sauvegarde des données permet de sécuriser les données en présence d'un « crash » système, un « crash » matériel ou une infiltration malveillante (hack), en les restaurant, presque à l'identique, dans leurs états originels. Dans le cadre d'une politique de sauvegarde, il est défini le rythme de la sauvegarde et le type de sauvegarde. À ce titre, il existe quatre types de sauvegardes développées. Tout d'abord, il existe la sauvegarde qualifiée de « totale » : celle-ci permet de sauvegarder dans sa totalité l'ensemble des fichiers, répertoires, systèmes de fichiers ou disques sélectionnés ; ensuite, la sauvegarde dite « incrémentale », celle-ci permet de sauvegarder uniquement les fichiers modifiés depuis la dernière sauvegarde totale ; puis, la sauvegarde que l'on appelle « différentielle » permet de sauvegarder tous les fichiers modifiés depuis la dernière sauvegarde lesquels vont être stockés dans ce que l'on appelle « des bandes de sauvegarde » ; enfin, la sauvegarde que l'on appelle « miroir », il s'agit d'une sauvegarde qui réalise une « copie » conforme des fichiers, laquelle s'effectue ponctuellement et prend en compte les données sources tel qu'elles existaient lors de la dernière sauvegarde[206]. En définitive, les mesures techniques que sont les sauvegardes permettent d'offrir des garanties non négligeables aux clients cloud, lesquelles sont la restauration ou la récupération des données dans le cloud. Le contrat de cloud computing doit, donc, prévoir les clauses relatives aux sauvegardes (déroulement, conditions et responsabilité).

---

[204] Concernant le détail des méthodes de chiffrement, Clé de chiffrement symétrique ou algorithme à clé secrète, Cryptographie asymétrique : https://www.kaspersky.fr/resource-center/definitions/encryption et https://www.techno-science.net/definition/6143.html : « un système de chiffrement est dit : « symétrique » quand il utilise la même clé pour chiffrer et déchiffrer ; « asymétrique » quand il utilise des clés différentes : une paire composée d'une clé publique, servant au chiffrement, et d'une clé privée, servant à déchiffrer. Le point fondamental soutenant cette décomposition publique/privée est l'impossibilité calculatoire de déduire la clé privée de la clé publique. Les méthodes les plus connues sont le DES, le Triple DES et l'AES pour la cryptographie symétrique, et le RSA pour la cryptographie asymétrique, aussi appelée cryptographie à clé publique ».

[205] Qu'est-ce que le chiffrement des données ? Définition et explication, Kaspersky, https://www.kaspersky.fr/resource-center/definitions/encryption. V. également, Chiffrement - Définition et Explications, techno-science.net : https://www.techno-science.net/definition/6143.html.

[206] Concernant la distinction des différents types de sauvegarde : https://www.netexplorer.fr/blog/quels-sont-les-differents-types-de-sauvegardes.

***68.*** Après avoir identifié les principales mesures techniques de sécurisation de l'infrastructure cloud et des données, il s'agit, à présent, d'envisager leurs mises en œuvre dans le contrat de cloud computing.

## B) La mise en œuvre des mesures techniques

***69.*** Afin d'envisager la mise en œuvre des mesures techniques pour la protection des données dans le cadre du contrat de cloud computing, il est nécessaire d'identifier quelles sont les réglementations applicables. Il convient d'envisager tant le cadre légal (1) que les sanctions en cas d'atteinte à ces mesures techniques (2).

### 1) Le cadre légal des mesures techniques

***70. Les données à caractère personnel.*** Dès lors que les données stockées dans le cloud computing concernent des données à caractère personnel, le RGPD[207] a vocation à s'appliquer. Il est précisé à l'article 32 dudit règlement que la protection des données personnelles nécessite de prendre des « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ». Cet article énonce les grands principes devant diriger la mise en place de ces mesures techniques de protection des données à caractère personnel. Il est précisé que ces mesures techniques et organisationnelles peuvent prendre la forme, « de la pseudonymisation et le chiffrement des données à caractère personnel ; des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ; des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ; une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement (…) »[208]. Parmi ces principes, il est possible d'identifier les principales mesures techniques de protection des données qui peuvent être résumées par la pseudonymisation, le chiffrement et les sauvegardes.

***71.*** Concernant la mise en œuvre de ces mesures techniques, il s'agit d'une obligation qui incombe au responsable du traitement et au sous-traitant qui doivent mettre en place les mesures

[207] Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[208] Article 32 du RGPD : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679.

techniques de protection et veiller au respect des règles de sécurité[209]. Afin de pouvoir justifier de la bonne mise en œuvre de ces mesures techniques et attester le niveau de sécurité approprié, le responsable du traitement et le sous-traitant pourront démontrer l'application d'un code de conduite approuvée ou d'un mécanisme de certification approuvé[210].

***72.*** Également, le RGPD énonce l'exigence du respect des principes de « Privacy by design » (protection des données dès la conception) et « Protection By Default » (protection des données par défaut). Le principe de la protection des données dès la conception impose aux entreprises publiques comme privées de prendre en compte les exigences relatives à la gestion et à la protection des données dès la conception des produits, services et systèmes exploitant des données à caractère personnel. Dans le cadre de la mise en application du RGPD, la CNIL a réalisé un guide rappelant les précautions élémentaires pour une gestion des risques constituée des quatre étapes et parmi elles, il est exigé de déterminer les mesures existantes permettant de traiter de chaque risque tel que le contrôle d'accès, les sauvegardes, la traçabilité, la sécurité des locaux, le chiffrement. Les données étant stockées dans le cloud (serveurs distants et reliés entre eux par une connexion internet), il faut, pour protéger ces données, mettre en place un système de sécurité des serveurs. La CNIL a établi des recommandations et en particulier invite à « limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées, utiliser des comptes de moindres privilèges pour les opérations courantes, adopter une politique spécifique de mots de passe pour les administrateurs, changer les mots de passe, au moins, lors de chaque départ d'un administrateur et en cas de suspicion de compromission, installer les mises à jour critique sans délai que ce soit pour les systèmes d'exploitation ou pour les applications, en programmant une vérification automatique hebdomadaire, effectuer des sauvegardes et les vérifier régulièrement, mettre en œuvre le protocole TLS (Transport Layer Security) ou un protocole assurant le chiffrement et l'authentification, au minimum pour tout échange de données sur internet et vérifier sa bonne mise en œuvre par des outils appropriés »[211]. La CNIL, également, préconise en matière d'administration de bases de données « d'utiliser des comptes nominatifs pour l'accès aux bases de données et créer des comptes spécifiques à chaque application ; de mettre en œuvre des mesures contre les attaques par injection de code SQL ("Structured Query Language" ou Langages de requêtes structurées), de scripts »[212]. Aujourd'hui, les mesures techniques se développent et se renforcent afin de

[209] Ibid.

[210] Ibid.

[211] CNIL, Sécurité : Sécuriser les serveurs, Renforcer les mesures de sécurité appliquées aux serveurs. https://www.cnil.fr/fr/securite-securiser-les-serveurs. V. également, Delmas-Linel B. et Mutz C., Les sept recommandations de la CNIL en matière de cloud computing : nécessaires mais pas suffisantes, RLDI 2012/85, nº 2871.

[212] Ibid.

sécuriser les données contre des attaques ou menaces de tiers. Outre le cadre légal applicable aux données à caractère personnel, d'autres textes viennent réglementer les mesures techniques pour permettre la protection des autres types de données.

***73. Les autres données.*** Au niveau européen, c'est la Directive européenne du 6 juillet 2016 qui établit le cadre légal concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union[213]. Cette Directive s'applique aux services de cloud computing[214] puisque la technologie du cloud fonctionne en réseau (serveurs distants et connectés entre eux par le réseau internet). S'agissant de ce texte, elle vient compléter la Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 (« Directive-cadre »)[215] laquelle concerne le secteur des réseaux de communication publics et services de communication électronique et vise les données à caractère personnel[216]. Ensuite, au niveau national, c'est la loi du 21 juin 2004 pour la confiance dans l'économie numérique[217] qui se charge d'intégrer dans l'ordre juridique interne les dispositifs relatifs aux moyens et prestations de protection technologique. Parmi ces moyens de protection technologique, de sécurité des réseaux et des systèmes d'information, nous retrouvons « la cryptologie » ou autrement appelé « le chiffrement ». Cette loi réglemente, par ailleurs, le régime de responsabilité des prestataires de moyens de cryptologie. En matière pénale, la loi du 15 novembre 2001 relative à la sécurité quotidienne[218] prévoit les conditions dans lesquelles « les prestataires de moyens de cryptologie pourront, dans certaines conditions, être tenus de remettre les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'ils ont fournies, voire de procéder eux-mêmes au déchiffrement »[219]. Par principe, les données sont cryptées afin de ne pas être lues par des tiers non autorisés. Cette disposition confère aux autorités publiques le droit d'exiger le décryptage de certaines données. Toujours dans l'identification des règles légales et spécifiquement celles applicables à l'exécution des

---

[213] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

[214] Ghueldre R. et Naftalski F., Le Lamy Assurances – Expert, Partie 5 E-commerce et assurance Titre 1 Distribution de l'assurance et Internet Chapitre 2 Commercialisation de l'assurance par Internet Section 1 Protection de l'internaute preneur d'assurance, 2 septembre 2021.

[215] Dir. Parl. Et Cons. CE nº 2002/21/CE, 7 mars 2002, JOCE 24 avr. 2002, nº L 108 concernant le cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre »).

[216] La Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifie la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs

[217] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique : L. nº 2004-575, 21 juin 2004, JO 22 juin.

[218] Loi du 15 novembre 2001 relative à la sécurité quotidienne : L. nº 2001-1062, 15 nov. 2001, JO 16 nov.

[219] Les articles 230-1 à 230-5 du Code de procédure pénale : dispositions permettant aux autorités judiciaires d'obtenir « la mise au clair des données chiffrées nécessaires à la manifestation de la vérité », c'est-à-dire d'informations inintelligibles ou cryptées.

services cloud, il est rappelé ici que la sécurité du cloud est un secteur réglementé. À ce titre, on a le référentiel ANSSI [220] du 30 juillet 2014 sur les prestataires de services sécurisés d'informatique en nuage, la norme ISO/IEC 27018 constituant les bonnes pratiques pour la protection des données personnelles dans les services de cloud, la norme ISO/IEC 27 017 en matière de sécurité du Cloud, la norme ISO 19086 sur la notion de niveau de service.

***74.*** Après avoir identifié le cadre légal général applicable aux mesures techniques, il est proposé, ici, d'étudier les sanctions en cas de manquements à ces règles.

**2) Les sanctions légales en cas d'atteinte aux mesures techniques**

***75.*** En cas d'atteinte à la sécurisation technologique de l'infrastructure cloud, des sanctions légales sont prévues, notamment, dans le Code pénal au chapitre III intitulé « *des atteintes aux systèmes de traitement automatisé de données* » « qui appréhende "l'intrusion"[221], le maintien volontaire dans un système[222], l'entrave volontaire au système[223], les atteintes volontaires aux données[224] et l'association de malfaiteurs en matière informatique »[225]. La loi sur la confiance dans l'économie numérique du 21 juin 2004[226] a, également, « créé un nouveau délit réprimant le fait, sans motif légitime, d'importer, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour

[220] ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information créée en 2009, qui dépend du Premier ministre : « Elle est l'autorité nationale en matière de sécurité des systèmes d'information » article du 3 du Décret n° 2009-834 du 7 juillet 2009.

[221] L'intrusion peut être caractérisée par l'introduction frauduleuse des données dans un système de traitement automatisé des données, celle-ci est pénalement répréhensible en application des dispositions de l'article 323-3 du code pénal : V. TGI Paris, 13e ch. Corr. 18 déc. 2014, no 12010064012, JurisData no 2014-032729 ; CCE 2015. Comm. 37, obs. É. A. Caprioli ; RSC 2015. 101, obs. J. Francillon.

[222] C. pén., art. 323-1 : V. également, TGI Paris, 12e ch., 17 déc. 2010, www.legalis.*net*, RLDI 2011/70, no 2316 concernant l'exploitation d'une faille informatique par un spécialiste, V. également, CA Paris, pôle 4, ch. 10, 5 févr. 2014, no 13/04833, Comm. Com. Électr. 2014, comm. 40 concernant la condamnation d'un internaute pour maintien frauduleux dans un système de traitement automatisé de données dès lors qu'il a constaté l'existence d'un contrôle d'accès et qu'il a réalisé des opérations de téléchargement de données protégées, opérations également constitutives de vol de fichiers informatiques.

[223] C. pén., art. 323-2 : « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende » : V. TGI Nanterre, 8 juin 2006, RLDI 2007/25, concernant une illustration de « *mailbombing* ».

[224] C. pén., art. 323-3 : « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende ».

[225] C. pén., art. 323-4 : « La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée ». V. Ghueldre R., Naftalski F., Le Lamy Assurances – Expert, Partie 5 E-commerce et assurance, titre 1 Distribution de l'assurance et Internet - Chapitre 2 Commercialisation de l'assurance par Internet, Section 1 Protection de l'internaute preneur d'assurance - Sécurité des transactions : cryptologie, lutte contre la fraude informatique, septembre 2021.

[226] L. no 2004-575, 21 juin 2004, JO 22 juin.

commettre les infractions précitées et renforce le *quantum* des peines prévues par les articles du Code pénal précités réprimant les atteintes aux systèmes de traitement automatisé de données »[227]. Par la suite, la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure[228] a créé une infraction d'usurpation d'identité en ligne. Il est, ainsi, puni d'un an d'emprisonnement et de 15 000 euros d'amende « le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération »[229]. Avant l'entrée en vigueur de ce texte, « l'usurpation d'identité était souvent appréhendée par la jurisprudence au titre de la violation du droit au respect de la vie privée et du droit à l'image »[230] . Les juges dans le cadre d'une affaire d'e-réputation ont, sur le fondement de l'article 226-4-1 du Code pénal, condamné une personne pour usurpation d'identité numérique[231]. En l'espèce, les juges ont considéré que la jeune femme s'était rendue coupable, entre autres, d'usurpation d'identité par la création de « multiples profils sur les réseaux sociaux en utilisant les noms exacts ou modifiés ou encore le pseudonyme » de son ex-concubin et de son ex-amant notamment, ainsi que leurs photos. Ayant également employé des propos injurieux à leur égard, les juges ont estimé que l'élément intentionnel du délit d'usurpation d'identité était caractérisé[232]. Par la suite, ce jugement a été confirmé par la Cour d'appel de Paris dans un arrêt du 13 avril 2016[233].

---

[227] Ghueldre R., Naftalski F., Le Lamy Assurances – Expert, Partie 5 E-commerce et assurance, titre 1 Distribution de l'assurance et Internet - Chapitre 2 Commercialisation de l'assurance par Internet, Section 1 Protection de l'internaute preneur d'assurance - Sécurité des transactions : cryptologie, lutte contre la fraude informatique, septembre 2021.

[228] Loi nº 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2 ; JO 15 mars 2011), V. Guerrier C., La LOPPSI 2 en 2011, RLDI 2011/70, nº 2325.

[229] V. C. pén. art. 226-4-1; pour une illustration v. CA Paris, 10 oct. 2014, nº 13/7387, Comm. Com. Élec. 2015, comm. 9, Caprioli E. : la cour d'appel de Paris a ainsi déclaré coupable du délit d'usurpation d'identité la personne qui utilise les coordonnées personnelles d'une autre pour créer de nouvelles adresses courriels et de nouveaux profils sur les réseaux sociaux dans le but de lui nuire ; V. aussi TGI Paris, 13e ch. Corr. 18 déc. 2014, nº 12010064012, relevant l'infraction d'usurpation d'identité et d'introduction frauduleuse de données dans une espèce où une personne avait profité d'une faille de sécurité sur le site internet officiel d'une personne publique, Comm. Com. Élec., 2015, comm. 37, Caprioli E..

[230] Illustration v. TGI Paris, 17e ch civ., 24 nov. 2010, www.legalis.net, CCE 2011, Lepage A., Faux profil sur Facebook, Comm. Com. Élec., 2011, comm. 28.

[231] TGI Paris, 24e ch. corr., 21 nov. 2014, RG nos 10183000010, 13311000700, min. publ., iVentures Consulting a. c/Mme L. A.; CCE 2015, comm. 85, obs. É.-A. Caprioli.

[232] Bensoussan A., Usurpation d'identité : 5 ans d'application de la LOPPSI 2, LEXING, 14 avril 2017 : https://www.alain-bensoussan.com/avocats/usurpation-identite-5-ans-loppsi-2/2017/04/14/.

[233] CA Paris, pôle 3, ch. 5, 13 avr. 2016, n°10183000010, L.A. c/min. publ., iVentures Consulting a. : « la cour d'appel de Paris a condamné à une peine de deux ans d'emprisonnement dont un an ferme une femme qui s'était rendue coupable de divers actes malveillants et de harcèlement à l'égard de deux de ses ex-compagnons et de leur entourage. La Cour a relevé que « les faits ont été commis durant de nombreux mois au préjudice de plusieurs victimes qui en ont été profondément affectées » et a ainsi condamné la jeune femme pour violence avec préméditation consistant en des messages électroniques à caractère injurieux et diffamatoire, usurpation d'identité par la création de fausses pages sur les réseaux sociaux diffusant des informations fausses et diffamatoires, appels téléphoniques malveillants et atteinte à l'intimité de la vie privée par fixation ou transmission de l'image d'une personne » : V. Féral-Schuhl C., Chapitre 712 - Atteintes aux systèmes d'information, Praxis Cyberdroit, 2020-2021

***76.*** En matière de données à caractère personnel, des sanctions peuvent, également, être encourues en cas d'atteintes aux droits des personnes concernées en application du RGPD[234]. Il existe également des règles spécifiques aux « opérateurs d'importance vitale »[235] qui sont soumis à titre d'exemple « à l'obligation de communiquer à l'ANSSI les incidents détectés dès qu'ils en ont connaissance, et de répondre aux demandes d'information de l'ANSSI[236]. En revanche, s'agissant des données à caractère personnel, toutes les entités ont l'obligation de notifier les violations de données à caractère personnel à la CNIL, et ce en application du RGPD. De manière complémentaire, il est possible d'appliquer les dispositions du Code pénal relatives aux délits de vol[237], d'escroquerie[238], d'abus de confiance[239], de destruction, dégradation ou détérioration de biens appartenant à autrui[240], de faux et d'usage de faux[241]. Par ailleurs, la modification de la Directive n° 2002/58/CE "concernant la protection de la vie privée dans les communications électroniques" par la directive n° 2009/136/CE du 25 novembre 2009[242] prévoit « au profit du fournisseur, une dispense de notification d'une violation des données à caractère personnel à l'abonné ou au particulier si le fournisseur a prouvé, à la satisfaction de l'autorité compétente, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. Ainsi, par la mise en place de telles mesures de protection technologique, les données sont rendues incompréhensibles aux tiers, lesquels ne sont pas autorisés à y avoir accès »[243].

---

[234] Art. 84 du RGPD ; également, C. pén., art. 226-16 à 226-24, V. Illustration de sanctions par la CNIL en présence d'un manquement à la sécurité : « elle a prononcé un avertissement le 9 janvier 2012 à l'encontre d'un hébergeur de données de santé, au sujet d'une déclaration mensongère contenue dans son dossier de demande d'agrément. La société prétendait chiffrer les données médicales hébergées, ce qui était inexact) ou communication à des tiers non autorisés, enregistrement ou conservation illicite de données à caractère personnel, détournement de finalité, divulgation illicite de données à caractère personnel ».

[235] Il s'agit d'une appellation introduite par la loi nº 2013-1168 du 18 décembre 2013, dite loi de programmation, aux articles L. 1332-1 et suivants du Code de la défense.

[236] Ghueldre R. et Naftalski F., F., Le Lamy Assurances – Expert, Partie 5 E-commerce et assurance, titre 1 Distribution de l'assurance et Internet - Chapitre 2 Commercialisation de l'assurance par Internet, Section 1 Protection de l'internaute preneur d'assurance - Sécurité des transactions : cryptologie, lutte contre la fraude informatique, septembre 2021.

[237] C. pén., art. 311-1 ; v. aussi arrêt de la Chambre criminelle portant sur le vol et le recel de fichiers clients d'un ancien employeur : Cass. crim., 20 oct. 2010, nº 09-88.387, inédit ; Caprioli E., Comm. Com. Élec., 2011, comm. 30.

[238] C. pén., art. 313-1.

[239] C. pén., art. 314-1 ; V ; illustration concernant le vol de données numériques : v. TGI Clermont-Ferrand, ch. Corr., 26 sept. 2011, Sociétés X.. et Y.. c/ Mme Rose, Légalis.net, 6 oct. 2011 ; CCE 2012, comm. n° 36, note E. A. Caprioli : qualification de vol et d'abus de confiance le fait pour une salariée de transférer le jour de son départ de l'entreprise, des données informatiques confidentielles afin de les utiliser à des fins personnelles.

[240] C. pén., art. 322-1 et 322-6.

[241] C. pén., art. 441-1.

[242] JOUE 18 déc. 2009, nº L 337 ; Cordier G., Focus sur la directive nº 2009/136/CE du 25 novembre 2009, RLDI 2010/57, nº 1904.

[243] Ghueldre R. et Naftalski F., F., Le Lamy Assurances – Expert, Partie 5 E-commerce et assurance, titre 1 Distribution de l'assurance et Internet - Chapitre 2 Commercialisation de l'assurance par Internet, Section 1 Protection de l'internaute preneur d'assurance - Sécurité des transactions : cryptologie, lutte contre la fraude informatique, septembre 2021.

***77. Le constat de l'insuffisance de la technologie pour assurer la protection des données dans le cloud et la dépendance de la technologie à la loi*** : En définitive, il apparaît qu'en dépit de l'existence des mesures techniques de protection des données, elles demeurent insuffisantes à elles seules puisque d'autres mesures techniques peuvent les contourner et « attaquer » l'infrastructure cloud. De ce constat, il apparaît que l'intervention du droit s'avère nécessaire pour dissuader les « pirates » par l'établissement de sanctions pénales et civiles. Dans ce sens, les mesures techniques sans l'établissement de mesures légales seraient insuffisantes à assurer la protection des données dans les contrats de cloud computing. La technologie est, ainsi, dépendante des mesures législatives et réglementaires en vigueur. Encore faut-il que les mesures légales soient constitutives d'un « droit dur » c'est-à-dire d'un droit contraignant[244]. Il apparaît, alors, fondamental de renforcer la protection des données par la loi et le contrat.

## II) L'étude de la protection des données par la loi et le contrat

***78.*** L'étude de la protection des données par la loi et le contrat est fondée sur une approche déductive et une analyse comparative des droits (A), et ce afin d'appréhender l'élaboration d'un cadre protecteur (B).

### A) Le cadre légal de la protection des données

Afin d'envisager la protection par la loi des données dans les contrats de cloud computing, il est fait le choix, ici, de fonder cette analyse des droits sur une approche déductive (1) et une analyse comparative (2).

#### 1) Une approche déductive

***79. La dichotomie des données*** : Il est fait le choix d'appréhender deux catégories de données, en distinguant la protection, d'une part, des données des personnes physiques (données à caractère personnel) et d'autre part les données des personnes morales de droit privé (données à caractère non personnel) dans les contrats de cloud computing. De cette étude, il apparaît que la loi prise dans son acception large dispose de lacunes afin de couvrir l'étendue des situations possibles

[244] V. *supra* n° 57.

lorsqu'une personne (physique ou morale) contractualise un service de cloud computing[245]. À ce titre, le Parlement européen avait exposé de manière explicite sa position quant à la nécessité selon lui « de bâtir une économie compétitive des données et de la connaissance en Europe (..) et insiste sur la nécessité d'accélérer le travail sur la normalisation de l'informatique en nuage ; souligne que de meilleures normes et une plus grande interopérabilité favoriseront la communication entre différents systèmes basés sur une infrastructure en nuage et permettront d'éviter les effets de dépendance vis-à-vis de fournisseurs pour les produits et les services d'informatique en nuage »[246].

***80.*** Il est constaté de prime abord que la réglementation protectrice[247] ne devrait pas s'appliquer au contrat de cloud computing puisque ce contrat n'a pas pour objet de traiter les données des utilisateurs du service de cloud computing[248]. Mais en pratique, il est constaté que le contrat de cloud prévoit la possibilité d'effectuer une collecte et un traitement de données. Dans une telle situation, la réglementation relative à la protection des données à caractère personnel à vocation à s'appliquer au contrat de cloud computing. Il s'agit, ici, d'étudier l'application de ces règles au contrat de cloud computing. Dans le cadre d'un contrat cloud entre un client, personne morale de droit privé, et un prestataire de services cloud, le règlement général à la protection des données ne s'applique pas aux données afférentes à la personne morale[249]. Il n'existe, donc, pas pour l'heure une réglementation spécifique à la protection des données des personnes morales équivalente à celle applicable aux personnes physiques concernant la protection de leurs données à caractère personnel. Il s'agit, alors, d'étudier les cadres légaux existants au niveau européen et étranger afin d'appréhender le niveau de protection accordé aux données des personnes morales dans le cadre d'un contrat de cloud computing.

---

[245] Bernault C., Informatique en nuage et données personnelles : quand l'informatique est dans les nuages, les données personnelles s'envolent ! RLDI 2012/78, nº 2616. V. également, Jouffin E., Recommandations de l'ABE en matière de cloud computing-Un texte mort-né ? revue Banque et Droit, 1er septembre 2018, numéro 181, page(s) 32-35.

[246] Commission européenne, Exploiter le potentiel de l'informatique en nuage en Europe, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions /* COM/2012/0529 final */.

[247] En particulier, la réglementation relative à la protection des données à caractère personnel : la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés laquelle définit les données à caractère personnel (dite loi informatique et libertés). La Convention 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (dit « RGPD » règlement général sur la protection des données).

[248] En principe, un contrat de cloud computing a seulement pour objet de mettre au profit d'une personne un espace de stockage de ses données dans le cloud (informatique en nuage).

[249] Considérant 14 du RGPD : « Le présent règlement ne couvre pas le traitement des données à caractère personnel qui concernent les personnes morales, et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale »

**2) Une analyse comparative**

***81. L'analyse d'un environnement juridique globalisé.*** Par environnement juridique, il s'agira d'étudier les cadres légaux existants au niveau européen et à l'étranger afin d'appréhender le niveau de protection accordée aux données lorsqu'elles font l'objet d'un contrat de cloud computing. La question étudiée est celle de l'effectivité du droit, en particulier la réglementation protectrice des données des personnes physiques et morales, dans un environnement globalisé. Comme l'indique Madame Morin-Dessailly, « pour les États-Unis, le contrôle de cette ressource [d'Internet] est devenu aussi fondamental que l'eau ou l'énergie. Elle est donc un enjeu majeur, tant sur le plan de la souveraineté que du développement de l'industrie américaine. Cet enjeu est tout aussi considérable pour l'Europe »[250]. Il apparaît que l'effectivité des règles de protection des données est remise en question en raison de l'hégémonie réglementaire étasunienne et la domination mondiale des États-Unis sur le marché de la « data »[251]. Cette hégémonie et cette domination sont perceptibles en matière de transfert de données et en matière de position monopolistique des plateformes de cloud computing[252]. Concernant la réglementation, la loi « Foreign Intelligence Surveillance Act (FISA) » du 25 octobre 1978 amendée par le FISA Amendements Act 2008, accorde le droit aux États-Unis de demander aux opérateurs tels que Facebook, Google de transmettre les métadonnées des européens collectées depuis le territoire de l'Union européenne [253] ; le « USA PATRIOT Act », loi antiterroriste qui a été adoptée le 26 octobre 2001 qui accorde la possibilité au gouvernement américain de mettre la main sur les données stockées sur les serveurs d'entreprises américaines ou basées aux USA, et, ce quel que soit le lieu où se trouvent effectivement ces données[254] ; la loi fédérale américaine dénommée "Clarifying Lawful Overseas Use of Data Act" ou « Cloud Act » par son acronyme promulguée le 23 mars 2018 laquelle est venue modifier « le chapitre 121 du Titre 18 du United States Code,

[250] C. Morin-Desailly, L'Union européenne, colonie du monde numérique ? Sénat, Rapport n° 443, 20 mars 2013.

[251] Ettighoffer D.-C., L'économique numérique sera-t-elle sous domination américaine ? Géoéconomie 2010/2 (n° 53), pages 89 à 99 : « La société française voit l'ensemble des référentiels géostratégiques et socio-économiques bouleversé par l'importante croissance de l'économie immatérielle, par la numérisation du monde et par la prolifération des réseaux. Alors que cette numérisation affecte les fonctions de production, de l'éducation, de la recherche, du commerce et de la distribution, sauronsnous maîtriser les infrastructures qui irriguent l'économie numérique alors que se profilent les développements prometteurs des applications du grid computing et du cloud computing ? Serons-nous une nation stratège dans ce nouveau monde de l'économie numérique alors que nous sommes loin de maîtriser les voies de navigation modernes du cyberespace ?(…) La globalisation numérique recouvre un monde socio-économique multipolaire bien déterminé à utiliser les réseaux électroniques pour se cultiver et s'enrichir. Autrefois, pour ce faire, on devait s'insérer dans les circuits commerciaux des biens.Face à l'enjeu majeur que représente la maîtrise des infrastructures qui maillent l'économie du futur, le fait que les Américains gouvernent Internet est moins la preuve de leur force que celle de notre propre faiblesse » : https://www.cairn.info/revue-geoeconomie-2010-2-page-89.htm.

[252] Andry F., Cloud et plateformes : pourquoi ces technologies ont-elles autant d'impact ? revue Dalloz IP/IT, publié le 1er juin 2020, numéro 6, page(s) 344-351.

[253] Traduction personnelle de la citation suivante : " The Foreign Intelligence Surveillance Act of 1978 prescribes procedures for requesting judicial authorization for electronic surveillance and physical search of persons engaged in espionage or international terrorism against the United States on behalf of a foreign power": https://fas.org/irp/agency/doj/fisa/).

[254] https://www.govinfo.gov/content/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf.

dénommé Stored Communications Act en permettant aux forces de l'ordre ou aux agences de renseignement américaines d'obtenir des opérateurs télécoms et des fournisseurs de services de Cloud computing des informations stockées sur leurs serveurs... Que ces données soient situées aux États-Unis ou à l'étranger » [255].

En partant du constat qu'il existe des lacunes légales en matière de protection des données dans les contrats de cloud computing, l'objectif de cette thèse est d'envisager les moyens juridiques permettant de remédier à ces lacunes et ainsi de contribuer au renforcement de la protection des données dans les contrats de cloud computing.

## B) Le renforcement de la protection par catégorie de données

***82.*** L'étude d'un cadre protecteur des données sera envisagée en distinguant les données à caractère personnel et les données des personnes morales de droit privé, lesquelles s'intègrent dans la grande catégorie des données à caractère non personnel.

***83. Le renforcement de la protection des données à caractère personnel.*** Afin d'élaborer un cadre légal pour le renforcement de la protection des données à caractère personnel des personnes physiques, une attention particulière sera portée à l'étude de la propriété des données. L'analyse a pour objet de déterminer si la notion de « propriété » est applicable aux données hébergées dans le cloud et peut permettre de renforcer la protection des données à caractère personnel. Également, il est question d'envisager la notion d'*un droit à l'autodétermination informationnelle* des personnes physiques pour le renforcement de la protection de leurs données à caractère personnel dans les contrats de cloud computing.

***84. Le renforcement de la protection des données des personnes morales.*** L'étude du renforcement de la protection des données des personnes morales au travers de la loi est envisagée en référence à la notion de *patrimoine informationnel numérique*[256]. L'analyse portera

[255] https://www.justice.gov/opa/press-release/file/1153446/download. V. Delmas-Linel B. et Mutz C., Le cloud computing à l'épreuve des souverainetés nationales. Faut-il avoir peur du USA Patriot Act ? », Lamy Droit de l'Immatériel, février 2013, p.53. V. Lavenue J.-J., Internationalisation ou américanisation du droit public : l'exemple paradoxal du droit du cyberspace confronté à la notion d'ordre public, Lex Electronica, Volume 11, Numéro 2,2006.

[256]Ces données sont regroupées dans ce que la doctrine nomme « le patrimoine informationnel » de la personne morale et a été utilisé initialement pour justifier l'exploitation de droits exclusifs : Saint-Aubin Th., les nouveaux enjeux juridiques des données (big data, web sémantique et linked data) Les droits de l'opérateur de données sur son patrimoine numérique informationnel, Revue Lamy Droit de l'Immatériel, N° 102, 1er mars 2014. Ce patrimoine informationnel a été défini comme étant comme « l'ensemble des données, protégées ou non, valorisables ou historiques, d'une personne physique ou morale » disposant « d'une valeur économique ou un intérêt stratégique, indépendamment du caractère protégeable ou non de ces informations par un droit de propriété intellectuelle» et correspond à «l'universalité des données détenues et produites par une personne physique ou morale, composante de son patrimoine immatériel : Galloux J.-C. « Ebauche d'une définition juridique de l'information », 1994, Dalloz chronique pp. 229-234.

sur l'identification et la consécration des droits pour la préservation de ce patrimoine informationnel numérique. Dans le cadre de l'étude du renforcement de la protection des données des personnes morales, il est envisagé d'analyser particulièrement les clauses du contrat de cloud computing qui sont susceptibles de porter atteinte aux droits des personnes morales pour la protection du patrimoine informationnel. Après avoir identifié ces clauses, il sera envisagé de procéder à des propositions de rédaction de clauses afin de renforcer la protection des données des personnes morales. Les propositions rédactionnelles porteront, tout d'abord, sur la sécurité technique avec les clauses relatives aux mesures techniques, la réversibilité ou le droit de portage des personnes morales ; puis, sur la sécurité juridique avec les clauses relatives à la confidentialité et l'interdiction de l'exploitation des données.

***85.*** **Plan.** Il est envisagé d'étudier, dans un premier temps, les lacunes existantes en matière de protection des données dans les contrats de cloud computing (PARTIE 1) puis dans un second temps, d'aborder les moyens permettant de compenser ces lacunes réelles et donc de renforcer la protection attendue (PARTIE 2).

# PARTIE 1 : Les lacunes de la protection des données dans les contrats de cloud computing

***86. La nécessité d'une adaptation des règles existantes à la protection des données dans le cloud computing.*** La réflexion entreprise sur la protection des données dans les contrats de cloud computing part du constat que les règles juridiques existantes nécessitent d'être adaptées à cette technologie. Le cloud computing est une technologie qui a pris son essor depuis plus d'une dizaine d'années et pourtant le droit n'a pas anticipé son évolution pour établir un cadre légal spécifique[257]. Qu'il s'agisse des données à caractère personnel (des personnes physiques), que des données des personnes morales (catégorie de données à caractère non personnel), la protection légale est assurée par l'application de règles non spécifiques au cloud computing. Dans cette partie, il est prévu d'étudier distinctement, les lacunes légales en matière de protection des données à caractère personnel et des données des personnes morales dans les contrats de cloud computing.

***87. Les lacunes légales en matière de protection des données à caractère personnel.*** Ces lacunes légales ont leurs sources dans l'absence d'une spécificité des règles à la matière du cloud computing et l'inaffectivité des règles européennes face à la réglementation étasunienne. La réglementation générale de la protection des données à caractère personnel (RGPD) ne devrait pas s'appliquer au contrat de computing, car il n'a pas vocation, en principe, à traiter les données des clients, personnes physiques. Mais en pratique cette réglementation va s'appliquer dès lors que le contrat cloud prévoit la collecte et le traitement des données à caractère personnel. Il est envisagé d'étudier l'application de cette réglementation à la protection des données à caractère personnel dans le cadre d'un contrat de cloud computing. En outre, il apparaît que ces lacunes légales résident, également, dans l'ineffectivité des règles européennes face à la réglementation étasunienne, laquelle est perceptible dans le cadre de transfert des données de l'Union européenne vers les États-Unis. En effet, les services de cloud computing sont très souvent des services transnationaux et suscitent des interrogations juridiquement complexes. Dans un contexte de mondialisation et de libre-échange au sein de l'espace économique européen (EEE), la difficulté consiste à établir un équilibre entre « la protection des données » et « la liberté de commerce et de l'industrie ». Pour préserver cet équilibre entre

[257] Basdevant A. et Mignard JP, l'empire des données - essai sur la société, les algorithmes et la loi, Don Quichotte éditions, mars 2018, p.173. V. également, Ettighoffer DC, L'économique numérique sera-t-elle sous domination américaine ? Géoéconomie 2010/2 (n° 53), pages 89 à 99 : « Serons-nous une nation stratège dans ce nouveau monde de l'économie numérique alors que nous sommes loin de maîtriser les voies de navigation modernes du cyberespace ? » : https://www.cairn.info/revue-geoeconomie-2010-2-page-89.htm.

« protection des données » et « liberté de commerce et de l'industrie », les États membres de l'Union européenne ont établi un cadre légal pour réglementer le transfert au sein de l'Union européenne et hors de l'Union européenne. Cette partie aborde, alors, la question de savoir si ce cadre légal permet d'assurer une protection suffisante des données à caractère personnel dans le cadre d'un contrat de cloud computing exécuté dans un contexte international. À ce titre, il est prévu d'étudier distinctement les règles relatives à un transfert de données au sein et hors de l'Union européenne afin d'identifier les lacunes légales.

***88. Les lacunes légales en matière de protection des données des personnes morales***. Il est rappelé que dans le cadre d'un contrat cloud entre un client, personne morale, et un prestataire de services cloud, le règlement général à la protection des données n'a pas vocation à s'appliquer aux données afférentes à la personne morale[258] puisqu'elles ne sont pas considérées comme étant des données à caractère personnel. Aujourd'hui, il n'existe pas pour l'heure une réglementation spécifique à la protection des données des personnes morales équivalente à celle applicable aux personnes physiques concernant la protection de leurs données à caractère personnel. Cette partie envisage l'étude des régimes applicables à la protection des données des personnes morales dans les contrats de cloud computing. Précisément, l'étude porte sur les cadres légaux européen et étranger applicables à la protection des données des personnes morales dans les contrats de cloud computing. Une attention particulière est accordée à la protection des données des personnes morales dans le cadre d'un transfert de données hors de l'Union européenne.

***89.*** **Plan de la partie 1** : Cette partie est dédiée à l'identification des lacunes légales en matière de protection des données à caractère personnel (Titre 1) et des données des personnes morales dans les contrats de cloud computing (Titre 2).

[258] Considérant 14 du RGPD : « Le présent règlement ne couvre pas le traitement des données à caractère personnel qui concernent les personnes morales, et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale ».

# Titre 1 : Les lacunes légales de la protection des données à caractère personnel dans les contrats de cloud computing

***90. L'étude du régime général applicable à la protection des données à caractère personnel.*** Cette étude met en lumière qu'il existe des lacunes légales en matière de protection des données à caractère personnel dans les contrats de cloud computing. Il est envisagé d'étudier l'application de la réglementation des données à caractère personnel au contrat de cloud computing, suivi d'une analyse critique de l'intégration d'une clause de collecte et de traitement des données dans les contrats de cloud computing.

***91. L'étude du régime du transfert des données.*** Dans cette partie, il convient de porter davantage la réflexion sur les transferts de données réalisés de l'Union européenne à destination de pays tiers. Les hypothèses de transfert au sein de l'Union européenne ne sont pas approfondies en raison de l'uniformisation des règles en la matière au sein de l'Union européenne. Le principe directeur pour le transfert des données au sein de l'Union européenne est la libre circulation des données. En revanche, il existe des interrogations concernant la protection des données à caractère personnel lorsque des transferts de données ont lieu de l'Union européenne à destination de pays tiers et notamment des États-Unis.

***92.* Plan du Titre 1** : Il est envisagé d'étudier, l'application au contrat de cloud computing, du régime général de la protection des données à caractère personnel (Chapitre 1) et du transfert des données hors de l'Union européenne (Chapitre 2).

# Chapitre 1 : L'application imparfaite du régime général de la protection des données à caractère personnel au contrat de cloud computing

***93. L'application de la réglementation générale des données à caractère personnel au contrat de cloud computing.*** La réglementation relative à la protection des données à caractère personnel (en particulier celle du RGPD) s'applique au contrat de cloud computing dès lors que le contrat prévoit une clause autorisant le prestataire de services cloud à collecter et à traiter les données à caractère personnel de ses clients, personnes physiques. En l'espèce, le prestataire de services cloud est qualifié par le RGPD de « responsable du traitement » dès lors qu'il collecte et traite des données à caractère personnel. Dans cette hypothèse, le prestataire de services de cloud computing est tenu au respect des prescriptions du RGPD et doit, donc, exécuter les obligations dévolues au responsable du traitement des données. Corrélativement à ces obligations, l'utilisateur de services cloud, personne physique, dispose de droits garantis par le RGPD pour la protection de ses données à caractère personnel. Il est question, alors, d'étudier quels sont *les droits garantis de la personne physique pour assurer la* protection de ses données à caractère personnel dans les contrats de cloud computing.

***94. L'inadaptation de la réglementation générale des données à caractère personnel au contrat de cloud computing***. L'instrument qu'est le RGPD n'est pas spécifique à l'usage de la technologie du cloud, mais est justifié en raison de l'intégration dans le contrat d'une clause autorisant le prestataire de services cloud à collecter et à traiter les données à caractère personnel de ses clients. Or, l'intégration d'une telle clause dans le contrat de cloud est critiquable. Ces critiques sont fondées, d'une part, sur les spécificités du contrat de cloud computing et d'autre part, sur les déséquilibres contractuels.

***95. Plan du chapitre 1*** : Afin d'apprécier les lacunes existantes en matière de protection des données à caractère personnel dans les contrats de cloud computing, il est question, tout d'abord, d'étudier l'application du régime général de la protection des données à caractère personnel au contrat de cloud computing (Section1) puis d'établir les critiques relatives à l'intégration d'une clause de collecte et de traitement des données dans les contrats de cloud computing (Section 2).

## Section 1 : L'identification des droits applicables au contrat cloud

***96.*** Cette partie est consacrée à l'identification des droits applicables à la protection des données à caractère personnel dans les contrats de cloud computing. L'étude porte sur l'application du droit à la protection des données à caractère personnel et du droit à la vie privée au contrat de cloud computing. Également, cette étude envisage les voies de recours dont dispose la personne physique en cas d'atteinte à ses droits à la protection des données à caractère personnel.

***97.*** **Plan**. Il est envisagé d'étudier l'application des droits fondamentaux (A) et les droits d'agir(B) au profit des personnes physiques pour la protection des données à caractère personnel dans les contrats de cloud computing.

### A) Le bénéfice des droits fondamentaux

***98.*** ***Le droit à la privée pour protéger les données à caractère personnel versus le droit à la protection des données à caractère personnel***. *Cette partie est consacrée à l'étude des droits généraux pour la protection des données à caractère personnel dans le contrat de cloud computing*. À titre liminaire, il est opportun de se poser la question de savoir si la protection des données à caractère personnel est reconnue comme étant un droit puis en cas de réponse positive identifier quelle est la nature de ce droit[259]. Pour assurer la protection des données à caractère personnel, il est utilisé deux fondements juridiques que sont le droit à la protection des données et le droit à la vie privée. Ces deux droits sont des droits fondamentaux et disposent d'une autonomie singulière l'un par rapport à l'autre. Ils ne doivent pas être confondus lorsqu'il s'agit de les appliquer à la protection des données à caractère personnel. Il est intéressant, en l'espèce, de s'interroger quelle a été la construction du droit à la vie privée pour l'appliquer au profit de la protection des données à caractère personnel dans les contrats de cloud computing. La notion de « droit à la vie privée » est définie par le Doyen Carbonnier comme étant « la sphère secrète de la vie où chacun aura le droit d'écarter les tiers » alors que « le droit à la protection des données personnelles assure quant à lui une protection indépendamment de toute violation du droit au respect de la vie privée ».

**Plan.** Cette distinction est, donc, marquée par leur fonction, le droit à la protection des données à caractère personnel (2) vise une protection a priori qui veille à empêcher la survenance d'un événement par le respect des conditions de licéité d'un traitement - consentement éclairé, usage

[259] Depuis la loi informatique du 6 janvier 1978 la protection des données à caractère personnel est un droit protégé et est expressément énoncé dans le RGPD que « la protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental ».

légitime pour une finalité déterminée (…). Au contraire, le droit au respect de la vie privée (1) constitue l'intrusion de la part des tiers. Il apparaît que malgré cette distinction de nature, ces deux droits tendent à un rapprochement perceptible dans l'étude de la jurisprudence relative à la protection des données à caractère personnel.

***1) L'application du droit à la vie privée à la protection des données à caractère personnel***

***99.*** Le droit fondamental à la vie privée est un fondement juridique applicable à la protection des données à caractère personnel. Ce fondement protège « certaines » informations dans le but de préserver la vie privée. Dans le cadre du droit à la vie privée, ces informations personnelles ont été définies par Monsieur Gutmann, comme « ces faits, communication ou opinions qui concernent l'individu et dont il serait raisonnable d'attendre de lui qu'il les considère comme intimes ou sensibles, et qu'il veuille en conséquence en empêcher ou au moins en restreindre leurs collecte, usage ou circulation »[260]. Le droit à la vie privée a été consacré dans de nombreux textes. L'article 8 de la Convention européenne des droits de l'Homme prévoit que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Ce droit englobe le droit à un nom, le droit au changement d'état civil et à une nouvelle identité, la protection contre les écoutes téléphoniques, la collecte d'informations à caractère privé par les services de sécurité d'un État et les publications portant atteinte à la vie privée. Ce droit permet aussi aux membres d'une minorité nationale d'avoir un mode de vie traditionnel »[261]. En France, le droit à la vie privée a été introduit dans les textes par la loi n° 70-643 du 19 juillet 1970 dont le principe est affirmé à l'article 9 du code civil qui dispose que « chacun a droit au respect de sa vie privée »[262]. Il s'est posé la question de savoir comment s'applique le « droit à la vie privée » à l'usage de l'informatique. À cette question, la loi du 6 janvier 1978 affirme expressément la nécessité que l'usage de l'informatique ne porte pas atteinte au droit à la vie privée ; ainsi elle dispose en ces termes que « l'informatique doit être au service de chaque citoyen. (…) Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »[263]. Malgré la

[260] Définition des informations de Gutmann D. qui a repris la définition d'un auteur américain Wacks dans Lepage A., Droits de la personnalité (Civ.), septembre 2009, dalloz, V. également Lepage A., Droits de la personnalité juillet 2006 - juillet 2007, Recueil Dalloz 2007 p. 2771.

[261] V. art. 8 de la Convention européenne des droits de l'Homme.

[262] V. art. 9 du Code civil.

[263] V. article premier de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifié par l'ordonnance n°2018-1125 du 12 décembre 2018.

consécration du droit à la vie privée dans de nombreux textes[264], il est apparu difficile de saisir les frontières du droit à la vie privée[265] en raison de l'absence d'une définition légale de la vie privée[266]. Pour compenser cette carence de définition, certains auteurs définissent le droit à la vie privée comme étant « la sphère secrète de la vie où chacun aura le droit d'écarter les tiers »[267]. Historiquement, c'est le juge qui, en présence d'un vide juridique, a précédé le législateur en se fondant sur l'ancien article 1382 du Code civil (aujourd'hui article 1240 du code civil) pour fonder ses décisions. Tel qu'affirmé par Monsieur Bamdé, ce vide juridique était donc comblé par « les rustines du droit de la responsabilité »[268]. Également, Monsieur Badinter considère que « le vide juridique qui existe en la matière est comparable à celui que l'on rencontre dans un trou noir »[269]. À la suite de la consécration du droit à la vie privée à l'article 9, la doctrine a observé que « l'application de cet article 9 a d'ailleurs donné une nouvelle impulsion à la jurisprudence, qui s'est livrée à une interprétation très dynamique de ses dispositions »[270]. En effet, l'article 9 est rédigé en des termes généraux, ce qui a permis aux juges d'interpréter ces dispositions pour rendre leurs décisions de justice. Il en résulte que ce droit à la vie privée est l'œuvre d'une construction prétorienne façonnée et complétée par l'article 9 du Code civil[271].

***100.*** Outre ce fondement civil, le droit à la vie privée dispose d'un fondement constitutionnel tel qu'il en ressort des décisions du Conseil Constitutionnel[272]. Il s'agit de l'article 2 de la

---

[264] Article 8 de la Convention européenne des droits de l'Homme : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Ce droit englobe le droit à un nom, le droit au changement d'état civil et à une nouvelle identité, la protection contre les écoutes téléphoniques, la collecte d'informations à caractère privé par les services de sécurité d'un État et les publications portant atteinte à la vie privée. Ce droit permet aussi aux membres d'une minorité nationale d'avoir un mode de vie traditionnel ». Également, V. article 9 du Code civil : « Chacun a droit au respect de sa vie privée ».

[265] Martin L., Le secret de la vie privée, RTD civ. 1959. 227, spéc. p. 230 : « Il paraît impossible, d'un mot, d'une formule, de dire à l'avance où finit la vie privée, où commence la vie publique. Il semble bien que cette question soit toujours dans la dépendance de l'appréciation souveraine des tribunaux ».

[266] Rapport Braibant sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, 3 mars 1998, Doc. fr., 1998.

[267] Carbonnier J., Droit civil des personnes, t.1,1996.

[268] Bamdé A., Docteur en droit privé de l'Université Paris 2 Panthéon-Assas, article électronique « L'émergence du droit des données à caractère personnel: de la loi informatique et libertés au RGPD », publié le 13 octobre 2018 : https://aurelienbamde.com/2018/10/13/lemergence-du-droit-des-donnees-a-caractere-personnel-de-la-loi-informatique-et-libertes-au-rgpd/.

[269] Badinter R., « Le droit au respect de la vie privée », JCP G, 1968, I, 2136, n°12.

[270] Malaurie Ph., Les précédents et le droit, Revue internationale de droit comparé, 2006 58-2 pp. 319-326 : au sujet de l'art. 9 C. civ. : « La jurisprudence avait suscité la loi, la loi a nourri la jurisprudence ».

[271] Basdevant A. et Mignard J-P., L'empire des données - essai sur la société, les algorithmes et la loi, Don Quichotte éditions, mars 2018, p.173.

[272] Décision du Conseil constitutionnel en date du 23 juillet 1999 : « La liberté proclamée par l'article 2 de la DDH qui dispose que le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme et que ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression, implique le respect de la vie privée » Cons. const. 23 juill. 1999, D. 2000. Somm. 265, obs. L. Marino, CCE 1999. Comm. 52, obs. R. Desgorces, RTD civ. 1999. 724, obs. N. Molfessis ; solution reprise dans la décision « loi relative au Pacs », nº 99-419 DC, 9 nov. 1999.

Déclaration des droits de l'homme et du citoyen (DDHC)[273] lequel dispose que « le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme et que ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression. Au niveau du droit international, l'article 12 de la Déclaration universelle des droits de l'homme affirme que « nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance ni d'atteinte à son honneur ou à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes »[274]. Par ailleurs, l'article 8 paragraphe 1er de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales énonce que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance »[275].

***101.*** Ce fondement juridique du droit à la vie privée est utilisé par les juges pour rendre des décisions de justice qui soient de nature à préserver la vie privée des personnes physiques. Concernant le sujet de la protection des données à caractère personnel, le Conseil constitutionnel a censuré l'article 5 de la loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité comme portant une atteinte au respect de la vie privée non proportionnée au but poursuivi[276]. Cet article prévoyait la création d'un traitement de données à caractère personnel facilitant le recueil et la conservation des données requises pour la délivrance du passeport français et de la carte nationale d'identité. Le Conseil, pour fonder sa décision, a relevé que, d'une part, ce fichier était destiné à recueillir des données relatives à la quasi-totalité de la population française et que d'autre part, que parmi les données recueillies, les données biométriques, notamment les empreintes digitales, sont des données particulièrement sensibles, et, enfin, que les caractéristiques techniques de ce fichier permettaient son interrogation à des fins autres que la vérification de l'identité[277]. Aujourd'hui, la personne doit être informée, au moment de la collecte des données, de la durée de conservation de celles-ci[278].

***102.*** Concernant l'application du droit privée à la protection des données à caractère personnel, certains auteurs, dont les sénateurs Madame Escoffier et Monsieur Détraigne considèrent que «

---

[273] La Déclaration des droits de l'homme et du citoyen (DDH) adoptée le 26 août 1789 et dont le Conseil constitutionnel a reconnu sa valeur constitutionnelle dans la décision n°71-44 DC du 16 juillet 1971 et 73-5 DC du 27 décembre 1973 : ainsi, la DDH est une norme de référence du contrôle de constitutionnalité exercé par le Conseil constitutionnel et dans la décision n°81-132 DC du 16 janvier 1982 relative à la loi de nationalisation, Rec. Cons. const. 18 ; AJDA 1982. 202, ces droits et principes ont « pleine valeur constitutionnelle ».

[274] Article 12 de la Déclaration universelle des droits de l'homme adoptée par l'Assemblée générale des Nations unies le 10 décembre 1948.

[275] Article 8 paragraphe 1er de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, adoptée par le Conseil de l'Europe le 4 novembre 1950 et ratifiée par la France en 1974 (JO 4 mai).

[276]DC, 22 mars 2012, n° 2012-652 DC, D. 2012. Actu. 623.

[277] Lepage A., Droits de la personnalité (Civ.), septembre 2009, dalloz.

[278] L. n° 78-17, 6 janv. 1978, art. 32, I, 8°, dans Lepage A., La protection contre le numérique : les données personnelles à l'aune de la loi pour une République numérique - Le droit civil à l'ère du numérique, actes du colloque du Master 2 Droit privé général et du Laboratoire de droit civil - Paris II - 21 avril 2017, La Semaine Juridique, Lexisnexis - Décembre 2017, page 38.

le droit à la protection des données à caractère personnel doit être regardé comme une déclinaison du principe de respect de la vie privée », rejetant ainsi l'idée selon laquelle la protection des données personnelles devrait être conçue « comme un droit autonome »[279]. En pratique, il existe une confusion opérée entre le droit à la vie privée et le droit à la protection des données à caractère personnel.

***103. Les critiques de la confusion opérée entre le droit à la vie privée et le droit à la protection des données à caractère personnel***. Cette confusion a été opérée dans la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique dont l'objet est de favoriser l'*open data*, renforcer la protection des citoyens dans la société numérique et l'accès au numérique pour tous. Il apparaît que dans son Titre II intitulé "La protection des droits dans la société numérique", le chapitre II est consacré à la "Protection de la vie privée en ligne" et c'est dans ce chapitre que figure la section consacrée à la "Protection des données à caractère personnel". La protection des données personnelles est, donc, incluse dans la partie dédiée à la vie privée en ligne. Sur ce point, A. Lepage a considéré que cette réforme « procède à un certain amalgame dont on peut regretter la confusion qu'il entretient, mais qui est révélateur de l'inspiration "personnaliste" de la présente réforme. En effet, les données à caractère personnel sont plus vastes que les informations relatives à la vie privée et quitte à ce qu'apparaisse un rapport d'inclusion, il serait plus logique de l'établir dans le sens inverse à celui exprimé par ce découpage de la loi du 7 octobre 2016. Il est toutefois plus rigoureux de considérer les données à caractère personnel et la vie privée comme des notions distinctes, objets de protections distinctes »[280]. Il résulte de cette observation que le droit à la protection des données à caractère personnel revêt un champ plus large que celui de la notion du droit à la vie privée[281].

***104.*** Bien qu'ayant une nature et un objet distinct, le droit à la vie privée est utilisé à titre de fondement juridique pour préserver « certaines » données à caractère personnel lesquelles se rattachent au cadre « privé » (intime) de la personne physique. Dès lors que le contrat cloud a pour objet le stockage de données à caractère personnel, la personne physique est en mesure d'utiliser le fondement du droit à la privée dans le cadre d'une action contre le prestataire de services cloud. À ce titre, la CJUE rappelle que «le règlement 2016/679 fournit, à ses articles 56 et 60 à 66, aux autorités de contrôle des États membres les instruments et les mécanismes qui

[279] Warusfel B. (sous la direction de Vivant M.), Le Lamy droit du numérique, Expert, Partie 3 - Numérique et contrats, division 3 - Les principaux contrats du numérique et leurs spécificités, chapitre 6 - Les contrats d'informatique dématérialisée (cloud computing), 22 avril 2022.

[280] Lepage A., La protection contre le numérique : les données personnelles à l'aune de la loi pour une République numérique - Le droit civil à l'ère du numérique, actes du colloque du Master 2 Droit privé général et du Laboratoire de droit civil - Paris II - 21 avril 2017, La Semaine Juridique, Lexisnexis - Décembre 2017, page 36.

[281] Ibid.

leur permettent, le cas échéant, de coopérer aux fins de parvenir à une décision commune fondée sur une mise en balance entre le droit de la personne concernée au respect de sa vie privée et à la protection des données à caractère personnel la concernant et l'intérêt du public de différents États membres à avoir accès à une information »[282]. En outre, elle précise dans ses décisions que « la protection du droit fondamental au respect de la vie privée exige, conformément à la jurisprudence constante de la Cour, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire»[283] et qu' « un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure, et ce en effectuant une pondération équilibrée entre, d'une part, l'objectif d'intérêt général et, d'autre part, les droits en cause »[284].

***105.*** Il en découle de ces affirmations que les données à caractère personnel doivent, être, « selon le cas, effacées ou rendues anonymes au terme des délais légaux »[285] afin de garantir la protection des données à caractère personnel et la vie privée des utilisateurs d'un service électronique. La CJUE établit un cadre pour l'application du principe de limitation de conservation des données; en rappelant que, lors d'un traitement ou d'un stockage des données « peuvent se présenter des situations dans lesquelles survient la nécessité de conserver lesdites données au-delà de ces délais aux fins de l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, et ce tant dans la situation où ces infractions ou ces atteintes ont déjà pu être constatées que dans celle où leur existence peut, au terme d'un examen objectif de l'ensemble des circonstances pertinentes, être raisonnablement soupçonnée»[286]. Si ces décisions affirment la nécessité de garantir aux personnes physiques la protection de leurs données à caractère personnel et leur droit à la vie privée, la CJUE rappelle que ces droits peuvent connaître des limitations. La CJUE rappelle la faculté qu'ont les États membres d'adopter des mesures législatives visant à limiter la portée de ces droits « lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale c'est-à-dire la sûreté de l'État, la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications

[282] CJUE 24 septembre 2019, Google LLC contre CNIL, C 507/17.

[283] CJUE, gde ch. 5 avril 2022, G.D. c/ Commissioner of An Garda Síochána et a., affaire n° C-140/20.

[284] CJUE 6 octobre 2020, La Quadrature du Net e.a., affaire n° C-511/18, C-512/18 et C-520/18.

[285] CJUE, gde ch. 5 avril 2022, G.D. c/ Commissioner of An Garda Síochána et a., affaire n° C-140/20.

[286] CJUE 6 octobre 2020, La Quadrature du Net e.a., affaire n° C-511/18, C-512/18 et C-520/18.

électroniques[287]»[288]. En définitive, le rappel de ces limitations par les juges permet d'encadrer l'application du droit à la vie privée à la matière de la protection des données à caractère personnel.

***106.*** Le développement des technologies informatiques fait naître de nouvelles craintes en matière de protection des données à caractère personnel. Face à ces nouvelles craintes, il a été considéré que le droit à la vie privée ne permet pas de protéger toutes les données à caractère personnel (uniquement celles qui concernent la vie privée) dans le cadre de l'utilisation des technologies informatiques et en particulier, ici, du cloud computing. En effet, G. Braibant a considéré dans son rapport que « la notion d'atteinte à la vie privée ne permet […] pas d'épuiser tous les cas de méconnaissance des droits des personnes auxquels la mise en œuvre de traitements de données à caractère personnel est susceptible de donner lieu »[289].

***2) L'application du droit fondamental à la protection des données à caractère personnel***

***107. Le cadre du droit fondamental à la protection des données*** : Le législateur, prenant conscience de l'existence des lacunes légales en matière de protection des données à caractère personnel dans le cadre d'une société où la technologie informatique prend de plus en plus de place, a adopté des dispositions. À ce titre, la loi informatique du 6 janvier 1978 modifiée par l'ordonnance du 12 décembre 2018 - énonce, à l'article 1er, que « l'informatique doit être au service de chaque citoyen. (…) Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »[290]. Cette loi modifiée consacre, ainsi, les droits de la personne physique pour la protection de ses données à caractère personnel. Il a été considéré par la doctrine que cette loi « se trouve être à la croisée de nombreuses libertés fondamentales, au-delà même du droit au respect à la vie privée »[291] et que

[287] Décision de la CJUE rendue dans l'affaire précitée (CJUE, gde ch. 5 avril 2022, G.D. c/ Commissioner of An Garda Síochána et a., affaire n° C-140/20.) concernant l'application dans l'ordre juridique irlandais de la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications.

[288] CJUE, gde ch. 5 avril 2022, affaire n° C-140/20, G.D. c/ Commissioner of An Garda Síochána et a.

[289] Braibant G., Rapport Données personnelles et société de l'information. Transposition en droit français de la directive numéro 95/46, La documentation française, coll. « rapports officiels », 1998, p. 7 ; V. également sur la notion d'atteinte à la vie privée, Beignier B., « Vie privée et vie publique », *Légipresse*, sep. 1995, n°124, pp. 67-74 ; d'Antin O., et Brossollet L., « Le domaine de la vie privée et sa délimitation jurisprudentielle » *Légicom*, octobre 1999, n° 20, pp. 9-19 ; Curto J., « La fin justifie-t-elle les moyens ? De la notion de vie privée et de la preuve déloyale » *Revue Lamy Droit Civil*, avr. 2012, n°92, pp. 55-56 ; dans Bamde A., Docteur en droit privé de l'Université Paris 2 Panthéon-Assas, article électronique « L'émergence du droit des données à caractère personnel: de la loi informatique et libertés au RGPD », publié le 13 octobre 2018 : https://aurelienbamde.com/2018/10/13/lemergence-du-droit-des-donnees-a-caractere-personnel-de-la-loi-informatique-et-libertes-au-rgpd/.

[290] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés » modifié par l'ordonnance n°2018-1125 du 12 décembre 2018.

[291] Lucas A., Devèze J., Frayssinet J., Droit de l'informatique et de l'Internet Collection « Thémis. Droit privé ». Presses Universitaires de France Paris, 2001.

les situations qui y sont appréhendées « s'étendent à tous les aspects de la vie publique et privée, des activités collectives et individuelles »[292].

***108.*** Si cette loi consacre les droits pour la protection des données à caractère personnel, la valeur de ce texte nous est donnée par le Conseil constitutionnel dans sa décision n° 92-316 du 20 janvier 1993 qui a considéré que « cette loi participe, avant tout, au système de protection de la liberté personnelle et individuelle »[293] ce qui, sans lui conférer une valeur constitutionnelle[294], « l'enracine en quelque sorte dans le bloc de constitutionnalité qui la vivifie »[295]. Après la promulgation de cette loi s'est, donc, posé la question d'établir un cadre transnational au niveau européen afin de garantir une certaine effectivité des législations nationales pour la protection des données à caractère personnel.

***109.*** Au niveau européen, il s'agissait de veiller à trouver un équilibre entre, d'une part, la protection des données à caractère personnel et, d'autre part, la libre circulation des données à caractère personnel[296]. Le 24 octobre 1995 est adopté la Directive européenne qui dispose, dans son dixième considérant, que : « […] le rapprochement des législations ne doit pas conduire à affaiblir la protection qu'elles assurent, mais, doit, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans la Communauté »[297]. L'article 1er du même texte énonce expressément l'exigence de la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère

---

[292] Laroque P., « Informatique et libertés publiques », in *Techniques de l'Ingénieur*, Fascicules H 8770, éd. Techniques, 1970.

[293] DC n° 92-316 du 20 janvier 1993, constitutionnalité du service central de prévention de la corruption et protection de la liberté individuelle en matière de fichiers informatiques, JORF n° 18 du 22 janvier 1993 p. 1118, Lucas A., Devèze J., Frayssinet J., note n° 100, n° 41, p. 28.

[294] Bamde A., Docteur en droit privé de l'Université Paris 2 Panthéon-Assas, article électronique « L'émergence du droit des données à caractère personnel: de la loi informatique et libertés au RGPD », publié le 13 octobre 2018 : https://aurelienbamde.com/2018/10/13/lemergence-du-droit-des-donnees-a-caractere-personnel-de-la-loi-informatique-et-libertes-au-rgpd/.

[295] Lucas A., Devèze J., Frayssinet J., Droit de l'informatique et de l'Internet Collection « Thémis. Droit privé ». Presses Universitaires de France Paris, 2001.

[296] Lors de la préparation d'un texte européen, le Conseil d'Etat s'est prononcé en assemblée générale, dans un avis du 13 juin 1993 et a indiqué que ce texte « ne saurait contenir de dispositions qui conduiraient à priver des principes de valeur constitutionnelle de la protection que leur accorde la loi du 6 janvier 1978 actuellement en vigueur » : V. Les grands avis du Conseil d'État, Paris, LGDJ, 1997, p. 399, note de Stirn B. ; Également, dans résolution de l'assemblée nationale du 25 juin 1993, il a été considéré que « la Communauté européenne ne peut « justifier son intervention dans la réglementation des traitements des données à caractère personnel qu'à la condition que la réalisation de cet objectif ne nuise pas au haut degré de protection dont doivent bénéficier les personnes physiques à l'égard de ces traitements et encore moins à assimiler ces données à de simples marchandises » : Bamde A., Docteur en droit privé de l'Université Paris 2 Panthéon-Assas, article électronique « L'émergence du droit des données à caractère personnel: de la loi informatique et libertés au RGPD », publié le 13 octobre 2018 : https://aurelienbamde.com/2018/10/13/lemergence-du-droit-des-donnees-a-caractere-personnel-de-la-loi-informatique-et-libertes-au-rgpd/.

[297] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO 23 nov. 1995, L. 281, pp. 31-50.

personnel[298]. Pour que cette Directive européenne puisse s'appliquer dans l'ordre juridique interne français, il a fallu la transposer dans l'ordre juridique interne. Une loi de transposition a, donc, été adoptée le 6 août 2004 dont les dispositions ont été intégrées à la loi du 6 juillet 1978. Par la suite, il a été adopté le RGPD[299] qui a abrogé la Directive de 1995 et est d'application directe dans l'ordre juridique interne français. En parallèle, en France, a été adoptée la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles qui est venue modifier la loi informatique du 6 janvier 1978 afin de se conformer au RGPD qui énonce expressément que « la protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental ». Également l'article 1er, deuxième paragraphe du RGPD affirme que « Le présent règlement protège les libertés et droits fondamentaux des personnes physiques, en particulier, le droit à la protection des données à caractère personnel ». Concernant cette affirmation, il faut relever que ce caractère de droit fondamental a été consacré dans les textes européens bien avant son inscription dans le RGPD[300]. Sur ce point, le caractère de droit fondamental à la protection des données a été expressément reconnu par plusieurs textes. L'article 8, paragraphe 1 de la Charte des Droits fondamentaux de l'Union européenne, affirme, alors, que « la protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental »[301]. Également, l'article 16, paragraphe 1 du Traité sur le fonctionnement de l'Union européenne dispose que « toute personne a droit à la protection des données à caractère personnel la concernant »[302]. Au niveau jurisprudentiel, la CJUE a, dans un arrêt du 18 juin 2020, rappelé que « le droit à la protection des données à caractère personnel consacré à l'article 8, paragraphe 1, de la Charte, qui est étroitement lié au droit au respect de la vie privée et familiale garanti à l'article 7 de la Charte, s'oppose à ce que des informations relatives à des personnes physiques identifiées ou identifiables soient diffusées à des tiers, qu'il s'agisse d'autorités publiques ou du public en général, à moins que cette diffusion intervienne en vertu d'un traitement loyal répondant aux exigences prescrites à l'article 8, paragraphe 2, de la Charte. En dehors de cette hypothèse, ladite diffusion, qui constitue un traitement de données à caractère personnel, doit donc être considérée comme

[298] Art. 1er, de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[299] Le règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE dit règlement général sur la protection des données (RGPD).

[300] Art. 1er, 2ème paragraphe du RGPD « Le présent règlement protège les libertés et droits fondamentaux des personnes physiques, en particulier leur droit à la protection des données à caractère personnel ».

[301] Art. 8 paragraphe 1 de la Charte des Droit Fondamentaux de l'Union Européenne.

[302] Art. 16 paragraphe 1 du Traité sur le fonctionnement de l'Union Européenne.

limitant le droit à la protection des données à caractère personnel garanti à l'article 8, paragraphe 1, de la Charte »[303].

***110. Les limites du droit fondamental à la protection des données.*** Si le caractère fondamental est incontesté, ce droit n'est pas absolu. À l'instar des autres droits fondamentaux, le droit à la protection des données à caractère personnel est limité par d'autres droits. À ce titre, il est rappelé, par le RGPD, que ce droit « doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité ». Lorsque ce droit fondamental est en confrontation avec un autre droit, lequel dispose d'une valeur fondamentale, il est fait usage du principe de proportionnalité, lequel variera en fonction des impératifs de protection et de l'époque concernée. Cette exigence de proportionnalité est énoncée également à l'article 52, paragraphe 1, de la Charte des droits fondamentaux. Sur ce point, la CJUE rappelle dans sa jurisprudence constante « qu'il ressort de l'article 52, paragraphe 1, de la Charte, notamment, que toute limitation apportée à l'exercice des droits et des libertés reconnus par la Charte doit répondre effectivement à des objectifs d'intérêt général reconnus par l'Union »[304]. Elle précise que « le droit à la protection des données à caractère personnel n'est pas un droit absolu ; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité. Le présent règlement respecte tous les droits fondamentaux et observe les libertés et les principes reconnus par la Charte, consacrés par les traités, en particulier le respect de la vie privée et familiale [...] la protection des données à caractère personnel, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise »[305]. En outre, le CEPD a adopté le 13 octobre 2021 des lignes directrices pour encadrer le recours à l'article 23 du RGPD qui énumère une liste de limitations aux droits des personnes concernées tels que la sécurité nationale, la défense nationale, la sécurité publique, la prévention et la détection d'infractions pénales (..), la protection de l'indépendance de la justice et des procédures judiciaires, des objectifs importants d'intérêt public général. Le CEPD précise le cadre de la mise en œuvre de ces limitations aux droits des personnes concernées. Pour être en conformité avec l'article 23 du RGPD, ces limitations « doivent être prévues par une mesure législative, concerner un nombre limité de droits des personnes concernées et/ou d'obligations du responsable du traitement, respecter l'essence des droits et libertés fondamentaux en cause, constituer une mesure nécessaire et

[303] CJUE 18 juin 2020, affaire n° C-78/18, commission européenne c/ Hongrie ; V. également en ce sens voir les arrêts CJUE du 9 novembre 2010, Volker und Markus Schecke et Eifert, C 92/09 et C 93/09, EU :C:2010:662, point 47, ainsi que du 24 novembre 2011, Asociación Nacional de Establecimientos Financieros de Crédito, C 468/10 et C 469/10, EU:C:2011:777, point 41 ; V. également CJUE 2 octobre 2018, Ministerio Fiscal, C 207/16, EU:C:2018:788, point 51.

[304] Ibid.

[305] Ibid.

proportionnée dans une société démocratique et sauvegarder l'un des motifs énoncés dans la liste exhaustive fixée à l'article 23 du RGPD (pt 9 des lignes directrices). Elles doivent en outre respecter les règles posées par la Charte des droits fondamentaux de l'Union européenne (art. 52) et la Convention européenne des droits de l'homme ». Au niveau des conditions, il est exigé que la mesure adoptée doit être suffisamment claire dans ses termes pour être prévisible, que le lien entre la restriction et l'objectif poursuivi soit explicite, qu'un test de nécessité et de proportionnalité doit être effectué au préalable, la mesure doit être appropriée à l'objectif poursuivi, qu'elle doit être étayée par des éléments de preuve décrivant le problème à traiter (…), la manière dont elle le traitera et pourquoi les mesures existantes ou moins intrusives ne peuvent pas le résoudre de manière suffisante. Il en résulte que toute restriction aux droits des personnes concernées doit être justifiée par des motifs, l'objectif poursuivi, le moment où la mesure est appliquée et le résultat du test de nécessité et de proportionnalité. Par ailleurs, une telle mesure restrictive des droits des personnes concernées ne peut qu'être temporaire et doit être levée à l'issue de l'objectif visé.

***111. Le droit fondamental à la protection des données, une déclinaison de droits***. Aujourd'hui, l'effectivité du droit à la protection des données se traduit par une déclinaison de droits, lesquels sont énoncés dans le RGPD. Pour garantir la protection des données à caractère personnel, la personne physique dispose du « droit à l'information »[306], du « droit d'accès aux données », d'un « droit de rectification »[307], d'un « droit à l'effacement » (ou « droit à l'oubli »)[308], un « droit à la limitation du traitement »[309], le « droit d'obtenir une notification concernant la rectification ou l'effacement de données, ou la limitation du traitement »[310].

***112.*** Cette déclinaison de droits qui est issue du droit fondamental à la protection des données n'a vocation à s'appliquer que dans l'hypothèse d'un traitement de données à caractère personnel. Tel qu'indiqué précédemment, un contrat de cloud computing n'a pas, en principe, pour objet de traiter les données de ses utilisateurs. En revanche, il est constaté, en pratique, que le contrat prévoit une clause de collecte et de traitement des données. Cette clause a pour objet d'accorder au prestataire de services cloud une autorisation de collecte et de traitement des données des clients. Dès lors que cette clause figure dans le contrat de cloud computing, le prestataire de services cloud est tenu d'appliquer les droits issus de la réglementation protectrice des données

[306] V. art. 13 et 14 du RGPD relatifs aux informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée.

[307] V. art.16 du RGPD.

[308] V. art. 17 du RGPD.

[309] V. art. 18 du RGPD.

[310] V. art. 19 et 20 du RGPD, permettant à la personne physique d'exiger de recevoir du responsable du traitement ses données dans un format adapté et structuré lui permettant de faciliter leurs transmissions à un autre responsable du traitement.

à caractère personnel. L'application de ces droits a une incidence directe sur le niveau de protection dont bénéficie le client, personne physique pour la protection de ses données à caractère personnel dans le cadre de l'exécution du contrat de cloud computing.

***113.*** En définitive, le droit fondamental à la protection des données à caractère personnel confère à la personne physique plusieurs types de droits pour assurer la protection de ses données à caractère personnel. Par ailleurs, il apparaît que ces droits garantis ne peuvent jouir d'une effectivité s'ils ne sont pas accompagnés de sanctions.

***114.*** Ainsi, après avoir étudié les fondements juridiques qui assurent une protection des données à caractère personnel, il est question désormais d'étudier l'application des droits d'agir au contrat de cloud computing.

## B) Le bénéfice des droits d'agir

***115.*** Pour assurer le respect des droits garantis par le RGPD, ce texte a prévu des sanctions pécuniaires, a mis en place un mécanisme de contrôle par les autorités administratives ainsi que la faculté pour tout un chacun de saisir les autorités administratives nationales compétentes pour statuer sur les manquements au RGPD. Cette partie a, ainsi, pour objet d'étudier les droits d'agirdont disposent les personnes physiques lorsqu'elles s'aperçoivent des atteintes à leurs données à caractère personnel dans le cadre de l'exécution d'un contrat de cloud computing.

***116.*** **Plan.** L'affirmation des droits d'agirse traduit par la faculté réservée aux personnes physiques d'introduire une action de groupe (1), une réclamation auprès d'une autorité de contrôle (2), le droit à un recours juridictionnel effectif (3) et le droit à la représentation (4).

### 1) Le droit à une action de groupe

***117.*** Les personnes disposent de la faculté du droit d'introduire une action de groupe appelée aussi « recours collectif »[311]. C'est la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle qui a créé une action de groupe visée aux articles 62 à 84[312], laquelle a été intégrée dans la loi du 6 janvier 1978 à l'article 37[313] ainsi que dans le RGPD à

[311] Consécration de l'action de groupe dans les textes : Loi n°2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle, Action de groupe (articles 62 à 84) ; Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : article 37 ; Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, Représentation des personnes en cas de recours (article 80).

[312] Loi n°2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle, Action de groupe (articles 62 à 84).

[313] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, v. article 37 et 43 ter.

l'article 80[314]. En ce temps, il s'agissait, donc, d'une « anticipation du Règlement général des données à caractère personnel du 27 avril 2016 (RGPD) »[315].

***118.*** L'objet de cette action de groupe est d'obtenir la cessation d'une atteinte au droit à la protection des données à caractère personnel ainsi que d'obtenir réparation du préjudice dès lors que les faits se sont produits après l'entrée en vigueur du RGPD soit le 24 mai 2018[316]. Dès lors que les personnes physiques ont subi le même préjudice découlant de l'atteinte au droit à la protection des données, causé par le même prestataire de services cloud alors elles pourront demander à une association de mettre en œuvre l'action de groupe[317]. C'est l'association[318] qui engage l'action de groupe au nom de toutes les personnes concernées et demande au nom de toutes les personnes concernées des dommages et intérêts au professionnel défaillant (responsable du traitement des données). En revanche, il est à noter que « malgré l'élargissement de son champ d'application, le bilan de cette nouvelle procédure est décevant : seules 21 actions de groupe ont été intentées depuis 2014, dont 14 dans le domaine de la consommation »[319].

***119.*** Concernant les effets de l'action de groupe, il y a une distinction lorsque le manquement a eu lieu avant ou après le 25 mai 2018 (date d'entrée en vigueur du RGPD). Avant le 25 mai 2018, la juge a, uniquement, la faculté d'ordonner la cessation de la violation des données personnelles. A compter du 25 mai 2018, outre la possibilité d'ordonner la cessation de la violation des données personnelles, le juge a, désormais, la faculté d'ordonner l'indemnisation des personnes rattachées à l'action de groupe (chaque personne est indemnisée individuellement) portant sur un préjudice matériel (exemple, une perte financière à la suite d'un vol commis à cause de la divulgation de vos données personnelles) ou moral (exemple, la réputation de la personne physique est atteinte à cause de la publication de données

[314] Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

[315] Lepage A., La protection contre le numérique : les données personnelles à l'aune de la loi pour une République numérique - le droit civil à l'ère numérique, Actes du colloque du Master 2 Droit privé général et du Laboratoire de droit civil - Paris II - 21 avril 2017, La Semaine Juridique, Lexisnexis – Décembre 2017, page 36 / V. not. Martial-Braz N., Les nouveaux droits des individus consacrés par la loi pour une République numérique. Quelles innovations ? Quelle articulation avec le règlement européen ? : Dalloz IP/IT, nov. 2016, p. 525 et s. - J.-L. Sauron, Le règlement général sur la protection des données, règlement (UE) n° 2016/679 du 27 avril 2016 : de quoi est-il le signe ? : Comm. com. électr. 2016, étude 16.

[316] V. art. 37, III, de la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. V. également, article 62 de la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXI$^{e}$ siècle.

[317] V. art. 37, II, de la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[318] Les conditions relatives à l'habilitation de l'association à exercer l'action de groupe : v. Article 37, IV, de la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; v. également, article 80 du RGPD concernant la représentation des personnes concernées.

[319] Rapport d'information de l'Assemblée nationale sur le bilan et les perspectives des actions de groupe présenté par les députés M. Philippe Gosselin et Mme Laurence Vichnievsky, n° 3085, 11 juin 2020.

personnelles)[320]. En matière de protection des données à caractère personnel, nous pouvons citer l'action de groupe intentée par UFC QUE CHOISIR contre Google le 26 juin 2019[321].

***120.*** Outre le droit d'introduire une action de groupe, il est possible d'introduire une réclamation auprès d'une autorité de contrôle.

**2) Le droit d'introduire une réclamation auprès d'une autorité de contrôle**

***121.*** La personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle[322] dès lors qu'elle considère que le traitement des données à caractère personnel la concernant constitue une violation du règlement[323]. En France, l'autorité de contrôle est la CNIL. À titre d'exemple, la CNIL a infligé le 21 janvier 2019, dans le cadre de son contrôle, une sanction de 50 millions d'euros à l'encontre de la société Google pour non-respect des obligations prévues au RGPD et en particulier pour manque de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité[324]. Cette sanction est intervenue à la suite d'un dépôt de plaintes collectives par l'association None Of Your Business (« NOYB ») et de l'association La Quadrature du Net (« LQDN ») qui reprochaient à Google de ne pas disposer d'une base juridique valable pour traiter les données personnelles des utilisateurs de ses services. La CNIL a procédé à un contrôle en ligne pour vérifier la conformité à la loi informatique et libertés et au RGPD des traitements de données personnelles réalisés par Google. Ce contrôle a été réalisé en analysant le parcours d'un utilisateur et les documents auxquels il peut avoir accès en créant un compte Google lors de la configuration de son équipement mobile sous Android. Sur la base de ce contrôle, la CNIL a constaté deux séries de manquements au RGPD. La première série est relative à un manquement aux obligations de transparence et d'information. Tout d'abord, la CNIL considérait que les informations fournies par Google n'étaient pas aisément accessibles pour les utilisateurs. La CNIL considérait que l'architecture générale de l'information ne permet pas de respecter les obligations du Règlement. Elle constate que les informations essentielles, telles que les finalités pour lesquelles les données sont traitées, la durée de conservation des données ou

[320] V. art. 37 de la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et pour la mise en œuvre du droit d'action. V. https://www.demarches.interieur.gouv.fr/particuliers/action-groupe-justice-cas-atteinte-aux-donnees-personnelles.

[321] V. *infra* n° 159 et 160 pour plus de détails concernant cette affaire.

[322] V. art. 13 du RGPD.

[323] V. art. 77 du RGPD.

[324] Décision du 21 janvier 2019 de la CNIL infligeant une sanction pécuniaire à l'encontre de la société Google pour manquement aux règles du RGPD : https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la.

les catégories de données utilisées pour la personnalisation de la publicité, sont de manière excessive disséminées dans plusieurs documents qui comportent des boutons et liens qu'il est nécessaire d'activer pour prendre connaissance d'informations complémentaires notamment sur la collecte de ses données ou la géolocalisation. Ensuite, la deuxième série de manquement est relative à l'absence de base légale pour réaliser les traitements de personnalisation de la publicité. Concernant ce manquement, Google invoque disposer du consentement de ses utilisateurs pour traiter leurs données à des fins de personnalisation de la publicité. Sur cet argument, la CNIL considère que le consentement n'est pas valablement recueilli pour deux raisons. Tout d'abord, le consentement des utilisateurs n'est pas suffisamment éclairé. L'information sur ces traitements, diluée dans plusieurs documents, ne permet pas à l'utilisateur de prendre conscience de leur ampleur. Par exemple, dans la rubrique dédiée à la « personnalisation des annonces », il n'est pas possible de prendre connaissance de la pluralité des services, sites, applications impliquées dans ces traitements (Google search, YouTube, Google home, Google maps, Playstore, Google photo…) et donc du volume de données traitées et combinées. Ensuite, la formation restreinte constate que le consentement recueilli n'est pas « spécifique » et « univoque » ». La CNIL a constaté que « lors de la création d'un compte, l'utilisateur a la possibilité de modifier certains des paramètres associés au compte en cliquant sur le bouton « plus d'options », présent avant le bouton « Créer un compte ». Il est notamment possible de paramétrer les modalités d'affichage des annonces personnalisées. Le RGPD n'est pas pour autant respecté ». Elle a justifié son point de vue en déclarant que « non seulement l'utilisateur doit faire la démarche de cliquer sur « plus d'options » pour accéder au paramétrage, mais en plus l'affichage d'annonces personnalisées est précoché par défaut. Or le consentement n'est « univoque », comme l'exige le RGPD, qu'à la condition que l'utilisateur effectue un acte positif (cocher une case non précochée par exemple). Enfin, avant de créer son compte, l'utilisateur est invité à cocher les cases « j'accepte les conditions d'utilisation de Google » et « j'accepte que mes informations soient utilisées telles que décrit ci-dessus et détaillées dans les règles de confidentialité » pour pouvoir créer son compte.

***122.*** Il en résulte, donc, que ce procédé conduit l'utilisateur à consentir en bloc, pour toutes les finalités poursuivies par Google sur la base de cet accord (personnalisation de la publicité, reconnaissance vocale, etc.). Or le consentement n'est « spécifique », comme l'exige le RGPD, qu'à la condition qu'il soit donné de manière distincte pour chaque finalité ». C'est pour ces raisons que la CNIL décide de condamner la société Google à une amende de 50 millions d'euros dont la décision a été rendue publique. Cette sanction paraît proportionnée compte tenu de l'ampleur des données que la société Google est amenée à traiter. Tel que rappelé par la CNIL, « malgré les mesures mises en œuvre par Google (documentation et outils de

paramétrage), les manquements constatés privent les utilisateurs de garanties fondamentales concernant des traitements pouvant révéler des pans entiers de leur vie privée, car reposant sur un volume considérable de données, une grande variété de services et des possibilités de combinaison de données quasi illimitées ». Cette décision nous permet d'identifier la grille d'analyse retenue par la CNIL pour apprécier la conformité aux obligations du RGPD. Il en découle que le consentement donné par l'utilisateur pour qu'il soit valide doit remplir les conditions suivantes ; il doit être « clair, spécifique et univoque ». Il est possible de transposer cette grille d'analyse aux conditions d'utilisations des services cloud pour apprécier si celles-ci sont conformes aux règles du RGPD.

**3) Le droit à un recours juridictionnel effectif**

***123.*** Outre le droit d'introduire une réclamation auprès d'une autorité de contrôle, la personne physique victime d'une atteinte à ses données à caractère personnel peut exercer un recours juridictionnel effectif contre, soit une autorité de contrôle, soit un responsable du traitement, soit un sous-traitant. La personne physique a, ainsi, la possibilité d'effectuer un recours juridictionnel contre une décision juridiquement contraignante d'une autorité de contrôle qui la concerne et qui porte atteinte aux droits dont elle dispose[325]. Pour exercer ce recours, elle doit intenter ce recours devant les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle est établie. Elle a, également, la possibilité d'exercer un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant dès lors qu'elle considère que les droits conférés par le règlement ont été violés du fait d'un traitement de ses données à caractère personnel[326]. Ce droit fait écho au droit fondamental à un recours effectif défendu par la Charte des droits fondamentaux[327]. Dans le cadre d'un contrat de cloud computing, il n'est pas aisé de déterminer le tribunal territorialement compétent pour connaître de ce type d'action. Concernant cette détermination, l'alinéa 2 de l'article 79 du RGPD apporte des précisions et énonce que « 2. Toute action contre un responsable du traitement ou un sous-traitant est intentée devant les juridictions de l'État membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement. Une telle action peut aussi être intentée devant les juridictions de l'État membre dans lequel la personne concernée a sa résidence habituelle, sauf si le responsable du traitement ou le sous-traitant est une autorité publique d'un État membre

[325] V. art. 78 du RGPD.

[326] V. art. 79 du RGPD.

[327] Article 47 de la Charte des droits fondamentaux de l'Union européenne, droit à un recours effectif et à accéder à un tribunal impartial.

agissant dans l'exercice de ses prérogatives de puissance publique »[328]. Par principe, l'action devra, donc, être intentée devant les juridictions de l'État membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement ou devant les juridictions de l'État membre dans lequel la personne concernée a sa résidence habituelle[329].

**4) Le droit à la représentation**

***124.*** Concernant les droits processuels, le RGPD affirme un droit à la représentation. Le droit à la représentation est le droit au profit de la personne physique de se faire représenter pour exercer son droit à réclamation et son droit à un recours juridictionnel effectif[330]. La personne physique concernée peut mandater un organisme, une organisation ou une association à but non lucratif pour qu'il introduise une réclamation en son nom et exerce les actions en son nom. Le droit à la représentation paraît fondamental pour que des professionnels spécialisés dans les problématiques de protection des données à caractère personnel puissent engager les actions adéquates en fonction de l'atteinte.

***125. L'analyse de l'application des droits d'agir au contrat de cloud computing***. En principe, les droits d'agirprévus par le RGPD n'ont pas vocation à s'appliquer au contrat de cloud computing sauf hypothèse où le contrat cloud prévoit une clause autorisant le prestataire de services cloud à collecter et à traiter les données de ses clients (personnes physiques). Dans cette hypothèse, le client a la faculté d'agir contre son prestataire de services cloud (pris en sa qualité de « responsable du traitement des données ») qui a porté atteinte à son droit à la protection des données à caractère personnel. Dans le cadre de l'exécution du contrat de cloud computing, les obligations qui sont mises à la charge du prestataire de services cloud sont celles dévolues au responsable du traitement des données. Ces obligations légales issues du RGPD vont perdurer tout le long de la relation commerciale (incluant la période de l'exécution du contrat de cloud computing) et postérieurement pendant toute la durée de la conservation des données.

***126.*** En conséquence, le client (personne physique) a la faculté d'agir contre le prestataire de services cloud (et éventuellement son sous-traitant) dès lors que ce dernier contrevient aux obligations prescrites par le RGPD pour la protection des données à caractère personnel.

[328] V. art. 79 du RGPD.

[329] Ibid.

[330] V. art. 80 du RGPD relatif au droit à la représentation des personnes concernées.

***127.*** En revanche, s'agissant de la protection des données stockées dans le cloud, on s'aperçoit très rapidement que cet instrument qu'est le RGPD se limite à la protection des données à caractère personnel et n'est pas spécifique à l'usage de la technologie du cloud.

## Section 2 : L'application critiquable des droits garantis au contrat de cloud computing

***128.*** Il apparaît, en pratique, que certains prestataires de services cloud insèrent dans les contrats de cloud computing des clauses les autorisant à collecter et à traiter les données à caractère personnel de leurs clients. Dès lors que ces clauses figurent dans le contrat de cloud computing, la réglementation des données à caractère personnel a vocation à s'appliquer.

***129.*** **Plan.** Il est envisagé de procéder, tout d'abord, à l'analyse critique de l'intégration d'une clause de collecte et de traitement des données dans les contrats de cloud computing (A) suivi de l'étude du déséquilibre contractuel (B).

### A) Le bénéfice des droits conditionné à une collecte et un traitement de données à caractère personnel

***130.*** **Plan.** Les critiques de l'intégration d'une clause de collecte et de traitement des données dans les contrats de cloud computing sont fondées, d'une part, sur les spécificités du contrat de cloud computing (1) et d'autre part, sur l'indétermination du périmètre contractuel de la clause de collecte et de traitement des données (2).

#### 1) Une collecte et un traitement injustifié au regard des spécificités du contrat de cloud computing

***131. La contestation de l'intégration de la clause de collecte et de traitement des données dans les contrats cloud au regard de l'objet du contrat de cloud computing***. L'intégration d'une clause de collecte et de traitement des données dans les contrats de cloud computing est contestable au regard de l'objet spécifique du contrat de cloud computing. Selon une appréciation rigoureuse, un contrat cloud a pour objet principalement la fourniture d'une prestation de services, au profit d'une personne, consistant en la mise à disposition d'un espace de stockage des données, et ce en optant pour un type d'infrastructure cloud (informatique en nuage). Par principe, aucune autorisation n'est accordée au prestataire de services cloud par le

client (personne physique) concernant le traitement et la collecte de ses données à caractère personnel. En pratique, il apparaît que les prestataires de services cloud et en particulier les « géants du numérique »[331] américain (les GAFA[332]), ont mis en place une stratégie contractuelle permettant d'une part, de collecter et d'exploiter les données à caractère personnel de leurs clients et d'autre part, d'obtenir une « certification » de conformité aux principes du RGPD.

***132.*** Si on considère qu'un contrat de cloud computing ne devrait pas prévoir une clause autorisant le prestataire de services à collecter et à traiter les données dans le cloud computing alors on aboutirait à l'exclusion de l'application du RGPD. Dans ce cas, quel serait le régime légal applicable à la protection des données à caractère personnel des utilisateurs, personnes physiques ? Il serait opportun de créer un régime juridique spécifique au cloud computing prévoyant les principes d'interdiction de traitement et d'exploitation des données. Cette proposition ne peut être accueillie favorablement puisque les acteurs publics tels que les États eux-mêmes et les acteurs économiques privés ont pris conscience des enjeux et des intérêts à collecter et à traiter massivement les données des personnes physiques. En raison des intérêts tirés de l'exploitation des données, nous assistons à l'introduction dans les contrats cloud, à destination des utilisateurs de personnes physiques, des clauses prévoyant la collecte et le traitement des données. Aujourd'hui, il n'existe aucune interdiction légale à ce qu'un contrat de cloud computing puisse prévoir une clause de traitement et de collecte des données. Le prestataire de services devra uniquement se conformer aux exigences du RGPD[333].

***133. La contestation de l'intégration de la clause de collecte et de traitement des données dans les contrats cloud au regard de la nature du contrat de cloud computing.*** Le contrat de cloud computing conclu entre un prestataire de services cloud et une personne physique est un contrat dit « standard », dans le sens que le contrat prévoit des dispositions identiques à une même catégorie de clients (ici, les personnes physiques). Dans le cadre d'un contrat de cloud computing dit « standard », les dispositions contractuelles sont imposées au client, personne

---

[331] L'expression « géants du numérique », désignent la quinzaine d'acteurs d'Internet d'envergure mondiale, dont (par ordre alphabétique) : Airbnb, Alibaba Group, Amazon, Apple, Booking.com, Facebook, Google, LinkedIn, Microsoft, Netflix, Twitter, Uber, Yahoo!. Ces multinationales partagent comme caractéristiques : d'avoir créé de volumineuses bases de données d'utilisateurs et, par conséquent, de produire un chiffre d'affaires considérable ; de rénover les applications de l'informatique en réseau, ouvertes vers le grand public sur le World Wide Web, par leur capacité d'innovation : https://fr.wikipedia.org/wiki/Géants_du_Web.

[332] L'acronyme GAFA « désigne quatre des entreprises les plus puissantes du monde de l'internet (et du monde tout court !) à savoir : Google, Apple, Facebook et Amazon. Ces firmes possèdent un pouvoir économique et financier considérable (parfois supérieur à un Etat). Par exemple, en 2015, les GAFA pesaient 1 675 milliards de dollars contre 1 131 milliards de dollars pour toutes les entreprises françaises cotées au CAC 40. On peut s'étonner de l'absence de Microsoft de ce "groupe", c'est pour ça qu'on trouve parfois l'acronyme GAFAM dans lequel le M représente Microsoft. Ces GAFA représentent l'économie du début du XXIe siècle et incarnent le passage à l'ère du digital » : https://www.glossaire-international.com/pages/tous-les-termes/gafa.html.

[333] Illustration : Le service cloud d'Apple dénomme « iCloud » permet « d'utiliser certains services Internet et de stocker vos données personnelles (telles que les contacts, calendriers, photos, notes, rappels, documents, données d'application et messagerie iCloud) et les rendre accessibles sur vos appareils et ordinateurs compatibles, et certains services de géolocalisation » https://www.apple.com/legal/internet-services/icloud/fr/terms.html.

physique, sans négociation et emportent, donc, la qualification de « contrat d'adhésion ». À titre d'exemple, le contrat icloud d'Apple mentionne expressément l'impossibilité de modifier ou de négocier les dispositions du contrat cloud[334]. En pratique, l'ensemble des contrats de cloud computing proposés par les prestataires de services de cloud computing aux personnes physiques sont des contrats d'adhésion[335].

***134.*** Concernant la formalisation de l'opération contractuelle du cloud computing, les Conditions d'utilisation des services cloud vont régir la relation contractuelle entre un prestataire de services cloud et l'utilisateur (personne physique). Ces Conditions d'utilisation constituent un contrat d'adhésion (les dispositions ne sont ni négociables ni modifiables). Malgré l'exigence de recueillir le consentement du client, personne physique, préalablement à la formation de tout contrat, il apparaît que les Conditions s'imposent « d'un bloc » au client et que le consentement semble donné de manière « tacite » et « non éclairée ». À titre d'exemple, il est précisé dans des Conditions d'utilisation de Google que « l'utilisation de nos Services implique votre acceptation des présentes Conditions d'utilisation [..] Vous devez respecter les règles applicables aux Services que vous utilisez »[336]. En l'espèce, le prestataire de services cloud estime que le consentement de l'utilisateur est recueilli dès lors que le client utilise le service cloud. Dans d'autres contrats cloud, le consentement est considéré avoir été donné par un simple « clic ». À titre illustratif dans les Conditions d'utilisation des services i-cloud d'Apple, il est expressément mentionné que « de cliquer sur "accepter" engendre l'application des présentes conditions à l'utilisateur dès lors qu'il y a eu un accès ou une utilisation du service i-cloud »[337]. Ce type de clause apparaît très souvent dans le cadre d'un contrat de prestations de services cloud dit « gratuit ». De l'étude de ces conditions, il résulte que le consentement donné de manière « tacite » et « non éclairé » ne peut être valide au regard des prescriptions du RGPD puisque ce texte exige à titre de validité que le consentement soit exprès, non équivoque et exprimé par une action positive, comme cocher une case à côté de laquelle est mentionnée la conséquence de l'acceptation des Conditions d'utilisation du service de cloud computing. Il en résulte que l'acceptation des Conditions d'utilisation des services cloud par l'utilisation des services cloud ou au moyen d'un clic peut être remise en cause.

---

[334] Dans le contrat i-cloud d'Apple la personne physique n'a pas la possibilité de demander de modifier ou d'aménager le contenu du contrat et Apple se « réserve le droit de modifier à tout moment le présent Contrat et d'imposer des conditions nouvelles ou supplémentaires concernant l'utilisation du Service » https://www.apple.com/legal/internet-services/icloud/fr/terms.html.

[335] Zolynski C., La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne, Dalloz IP/IT 2020 p.429.

[336] Les conditions d'utilisation du service cloud de Google : https://policies.Google.com/terms.

[337] Les conditions d'utilisation des services i-cloud d'Apple : https://www.apple.com/legal/internet-services/icloud/fr/terms.html.

***135.*** Après avoir étudié que l'intégration de la clause de collecte et de traitement dans un contrat de cloud computing est injustifiée au regard de l'objet et de la nature du contrat, il est, question, à présent d'étudier le périmètre contractuel de cette clause.

**2) L'indétermination du périmètre contractuel de la clause de collecte et de traitement des données**

***136. La difficile identification de la donnée à caractère personnel pour la collecte et le traitement des données***. Pour permettre au prestataire de services cloud de collecter et de traiter les données personnelles de ses clients, il leur est demandé de créer « un compte client ». La question se pose de savoir de quelle manière est associée « la donnée » à l'identité de l'utilisateur dans le cas où l'utilisateur déciderait de ne pas créer de compte personnel. Dans cette hypothèse, la donnée collectée est associée à des identifiants uniques liés au navigateur ou à l'application utilisée par l'utilisateur du service cloud[338]. Il s'agit, ensuite, de savoir si cette identification à travers le navigateur pouvait constituer une donnée à caractère personnel. La CJUE[339] s'est prononcée sur la question préjudicielle relative à la conservation des adresses IP[340] au terme d'une consultation d'un site internet au regard de la directive européenne de 1995[341]. Il en ressort que la qualification de ces données à caractère personnel devrait dépendre du point de savoir si la personne physique est rendue identifiable. À ce sujet, la Cour fédérale de justice met en lumière la controverse doctrinale concernant les critères d'identification de la personne physique qui se fonde sur un critère soit « objectif » soit « relatif »[342]. L'application d'un critère « objectif » aboutit à la conséquence que les données telles que les adresses IP pourraient être considérées comme revêtant un caractère personnel même si seul un tiers est en mesure de déterminer l'identité de la personne concernée. Selon un critère « relatif », l'adresse IP pourrait être considérée comme étant à caractère personnel à l'égard d'un organisme, tel que le fournisseur d'accès à internet, puisqu'elle permet l'identification précise de l'utilisateur, mais comme ne revêtant pas un tel caractère à l'égard d'un autre organisme, lequel ne dispose pas d'autres éléments nécessaires à son identification. En l'espèce, il s'agissait de savoir si l'adresse dynamique prise en combinaison avec la date de la session à laquelle elle se rapporte constitue

[338] Les règles de confidentialité et conditions d'utilisation des services de Google : https://policies.Google.com/privacy.

[339] CJUE 19 octobre 2016, affaire n° C-582/14, M. B. / Bundesrepublik Deutschland, JO 1995, L 281, p. 31. La CJUE s'est prononcée sur la question préjudicielle émise par la Cour fédérale de justice d'Allemagne concernant de l'article 2, sous a), et de l'article 7, sous f), de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[340] Internet Protocol.

[341] Art. 7, sous f), de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31).

[342] CJUE 19 octobre 2016, affaire n° C-582/14, M. B. / Bundesrepublik Deutschland, JO 1995, *op. cit.*.

une donnée à caractère personnel. À cette question, la CJUE a considéré, en application de l'article 2, sous a), de la directive européenne du 24 octobre 1995[343], « qu'une adresse de protocole internet dynamique enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site internet que ce fournisseur rend accessible au public constitue, à l'égard dudit fournisseur, une donnée à caractère personnel au sens de cette disposition, lorsqu'il dispose de moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à internet de cette personne »[344]. En se fondant sur cette décision, une adresse IP peut dans certains cas être caractérisée comme une donnée à caractère personnel. En France, la première chambre civile de la Cour de cassation dans un arrêt en date du 3 novembre 2016[345] considère depuis que « les adresses IP, qui permettent d'identifier indirectement une personne physique, sont des données à caractère personnel, de sorte que leur collecte constitue un traitement de données à caractère personnel et doit faire l'objet d'une déclaration préalable auprès de la CNIL[346] ». Par cette décision, la Cour de cassation tranche et affirme ainsi que l'adresse IP est une donnée à caractère personnel. Cette position vient conforter les décisions prises auparavant par le Conseil constitutionnel[347], par le Conseil d'État[348] et par la Cour de justice de l'Union européenne[349], laquelle a qualifiée de donnée à caractère personnel l'adresse IP dynamique, attribuée à chaque connexion à internet et remplacée lors de connexions ultérieures[350]. Ensuite, si l'utilisateur dispose d'un compte et se connecte à partir de « son compte » dans ce cas la donnée ainsi collectée est rattachée à son compte et est donc considérée comme une donnée à caractère personnel puisque ce rattachement a pour effet de l'identifier personnellement.

---

[343] En application de « l'article 2, sous a), de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[344] CJUE 19 octobre 2016, affaire n° C-582/14, M. B. / Bundesrepublik Deutschland, JO 1995, L 281, p. 31. La CJUE s'est prononcée sur la question préjudicielle émise par la Cour fédérale de justice d'Irlande concernant de l'article 2, sous a), et de l'article 7, sous f), de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[345] Cass. 1re civ., 3 nov. 2016, pourvoi n° 15-22.595, JurisData n° 2016-022669, JCP G 2016, 1310, R. Perray.

[346] Depuis l'entrée en vigueur, les données à caractère personnel ne font plus l'objet d'une déclaration préalable auprès de la CNIL.

[347] DC n° 2009-580 du 10 juin 2009, constitutionnalité de la loi favorisant la diffusion et la protection de la création sur internet, JurisData n° 2009-024431 ; JCP G 2009, 101, J.-Ph. Feldman.

[348] CE, 10e et 9e ss-sect. réunies, 12 mars 2014, n° 353193, JurisData n° 2014- 004444.

[349] CJUE, 19 octobre 2016, affaire n° C-582/14, Breyer c/ Bundesrepublik Deutschland : JurisData n° 2016-030407. – V. déjà en ce sens, au sujet des adresses IP statiques, CJUE, 24 novembre 2011, affaire n° C-70/10, Scarlet Extended SA c/ Sté belge des auteurs, compositeurs et éditeurs : JurisData n° 2011-032131 ; Comm. com. électr. 2012, comm. 63, obs. A. Debet ; Rev. sc. crim. 2012, p. 163, obs. J. Francillon.

[350] Lepage A., La protection contre le numérique : les données personnelles à l'aune de la loi pour une république numérique – le droit civil à l'ère numérique, actes du colloque du master 2 droit privé général et du laboratoire de droit civil – paris II – 21 avril 2017, la semaine juridique, lexisnexis – décembre 2017 page 35.

***137.*** Pour prévoir les hypothèses relatives à la création ou non d'un compte client, le prestataire de services cloud définit dans la politique de confidentialité ce qu'il faut entendre par « donnée à caractère personnel », par exemple, il est indiqué qu'il peut s'agir du nom, de l'adresse postale, du numéro de téléphone (..). Très souvent, le champ de cette définition est volontairement restreint afin de limiter le plus possible l'application du RGPD aux données collectées et exploitées par le prestataire. Une vigilance doit être portée sur le contenu de la définition des données à caractère personnel dans les contrats de cloud computing, puisque de ce contenu il en découlera l'application ou non par le prestataire du RGPD. À l'inverse dans le RGPD, la définition des « données à caractère personnel »[351] est volontairement large afin de permettre une application, la plus étendue possible, du texte et donc de la protection des données.

***138. Un champ d'application indéterminé de la clause autorisant la collecte et le traitement des données***. Le contrat cloud peut prévoir que l'utilisateur concède au fournisseur une licence pour collecter et traiter les données. S'agissant des données collectées, les "Conditions d'utilisation du service cloud" doivent les identifier expressément[352]. Dans de nombreux contrats, la clause de collecte et de traitement est rédigée de manière "large" et dispose d'un champ d'application très étendu. À titre d'exemple, Google énonce dans son contrat cloud à destination de personnes physiques que « lorsque vous importez, soumettez, stockez, envoyez ou recevez des contenus à ou à travers de nos Services, vous accordez à Google (et à toute personne travaillant avec Google) une licence, dans le monde entier, d'utilisation, d'hébergement, de stockage, de reproduction, de modification, de création d'œuvres dérivées (des traductions, des adaptations ou d'autres modifications destinées à améliorer le fonctionnement de vos contenus par le biais de nos Services), de communication, de publication, de représentation publique, d'affichage public ou de distribution publique desdits contenus »[353]. Cette clause à un champ d'application tellement large qu'il paraît difficile de déterminer avec précision l'étendue des droits de Google pour le traitement des données des clients. En définitive, la clause autorisant le prestataire de services cloud à collecter et à traiter les données nécessite une attention particulière des utilisateurs qui doivent être informés des conséquences de l'utilisation des services cloud quant à l'usage qui peut en être fait de leurs données à caractère personnel[354].

---

[351] Art. 4 du RGPD : il s'agit de « toute information se rapportant à une personne physique identifiée ou identifiable (…) ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

[352] Les conditions d'utilisation des services i-cloud d'Apple : https ://www.apple.com/legal/internet-services/icloud/fr/terms.html.

[353] Clauses issues des Conditions de services dans le contrat cloud de Google à destination de personnes physiques : https://policies.Google.com/terms.

[354] Les conditions d'utilisation du service cloud de Google : https://policies.Google.com/terms.

***139. La justification de la collecte et du traitement des données par des indicateurs imprécis***. Pour délimiter le champ d'application de la clause de collecte et de traitement des données, certains prestataires de Services cloud dont Google mentionnent que cette licence a pour limite l'exploitation, la promotion, l'amélioration ou le développement des services. Autrement dit, Google devrait utiliser son droit de collecte et de traitement des données dans le cadre limité de l'exploitation, la promotion, l'amélioration ou le développement des services[355]. Bien qu'elle ait pour objet de fixer des limites au droit de collecte et de traitement des données, cette clause ne permet pas au client de connaître précisément le périmètre des données pouvant faire l'objet d'une collecte et d'un traitement. Si l'on compare avec les Conditions de la société Apple, il apparaît que la clause autorisant la collecte et le traitement des données est plus encadrée. À titre illustratif, il est énoncé qu'Apple « est susceptible, avec la permission de l'utilisateur, de traiter les données à caractère personnel dans des cas précis ; tels que le respect d'une obligation juridique, l'exécution d'un contrat auquel est parti l'utilisateur, protéger les intérêts légitimes d'Apple, pour créer, développer les produits, services, à des fins de sécurité de compte et de réseau, vérifier l'identité de l'utilisateur, pour envoyer des avis importants, pour administrer ces programmes »[356]. En vue de légitimer la collecte et le traitement des données par les prestataires de services cloud, il est avancé l'argument par ces derniers que les informations ainsi collectées contribuent à l'amélioration des services proposés aux utilisateurs du service cloud. Il apparaît que cette indication est imprécise et qu'elle est susceptible de porter atteinte au droit à la protection des données à caractère personnel des utilisateurs d'un service cloud. En effet, il est tout à fait possible de faire tout type d'usage des données sous couvert de l'exploitation, la promotion, l'amélioration ou le développement des services proposés par le prestataire de services cloud. Bien que cette licence soit consentie par le client, personne physique, au prestataire de services cloud, la validité du consentement pourrait être remise en cause en raison de la généralité et de l'imprécision de cette clause.

***140. L'utilisation critiquable de la notion de « propriété » dans la clause autorisant la collecte et le traitement des données***. Dans le cadre de l'étude de cette licence (clause autorisant le prestataire de services cloud à collecter et à traiter les données à caractère personnel), il est intéressant d'identifier les prérogatives des prestataires concernant le traitement des données de leurs clients. Certains prestataires de services cloud mentionnent dans leurs Conditions d'utilisation de services cloud que l'utilisateur demeure « propriétaire » de ses données. Il est,

[355] Ibid.

[356] Le contrat i.cloud d'Apple : https ://www.apple.com/legal/privacy/fr-ca/.

ainsi, mentionné dans les Conditions d'utilisation de Google que « vous restez propriétaire des données que vous nous confiez et nous pensons qu'il est important que vous puissiez y accéder »[357]. En l'espèce, l'utilisateur serait « propriétaire » de ses données et le prestataire de services cloud serait une sorte de « garant » à qui les données ont été confiées. Cette mention emporte des critiques puisque le fait de confier des données implique la restitution à l'identique sans altérations des données. Le prestataire de services cloud est, ici, autorisé à exploiter les données et cette exploitation engendre de facto une atteinte à l'intégrité des données. En outre, il en résulte que même si les données sont restituées à son « propriétaire », il n'en demeure pas moins que d'autres copies peuvent exister dans d'autres serveurs qui continueront à être utilisées par le prestataire de services cloud lui-même ou d'autres organisations.

***141. L'existence critiquable d'une collecte de « masse » des données dans les contrats cloud « gratuit ».*** Dans le cadre de l'étude de la politique de confidentialité (notamment celle de Google), il est constaté que si la collecte des données semble concerner uniquement des données techniques[358], celle-ci permet en réalité de détenir et d'exploiter les informations rattachées à la personne la rendant identifiable. La collecte des données techniques se poursuit avec les données relatives à l'activité des utilisateurs des services cloud, telle que les termes recherchés, les vidéos consultées ou regardées, les données audio et vocales lors de l'utilisation des fonctionnalités audio, les données relatives à l'identification des personnes avec lesquelles il y a eu une communication ou un partage de contenu, les données relatives à l'historique de navigation. La collecte apparaît plus « déroutante » lorsqu'un utilisateur recourt aux services cloud de Google « pour passer et recevoir des appels ou pour envoyer et recevoir des messages »[359]. À cela, Google indique qu'elle est susceptible « de collecter des informations relatives aux communications téléphoniques, comme votre numéro de téléphone, celui de l'émetteur, celui du destinataire, les numéros de transfert, l'heure et la date des appels et des messages, la durée des appels, les données de routage et les types d'appels »[360]. Il est indiqué que Google collecte les données relatives à la géolocalisation des utilisateurs des services cloud, en se servant du GPS, de l'adresse IP, des données de capteurs de l'appareil, les points d'accès Wi-Fi, des antennes-relais et des appareils sur lesquels le Bluetooth est activé. Sur ce point, il est tout de même laissé, à l'utilisateur, la possibilité d'activer ou de désactiver la position géographique de l'appareil Android. Par ailleurs, il apparaît que Google collecte « activement » les données de ses utilisateurs depuis des sources accessibles publiquement. À ce titre, il est

[357] Les conditions d'utilisation du service cloud de Google : https://policies.Google.com/terms.

[358] Les règles de confidentialité et conditions d'utilisation des services de Google : https ://policies.Google.com/privacy.

[359] Ibid.

[360] Ibid.

mentionné que « si votre nom est mentionné dans votre journal local, le moteur de recherche Google est susceptible de répertorier l'article en question et de l'afficher dans une recherche effectuée sur votre nom par d'autres utilisateurs »[361].

***142.*** Pour procéder à cette collecte de « masse » des données des utilisateurs de services cloud, Google se sert de plusieurs technologies tel que « les cookies, les tags de pixel, les éléments stockés en local (tels que le stockage sur les navigateurs web ou les caches de données d'application), les bases de données et les fichiers journaux de serveur »[362]. La justification apportée à cette collecte de « masse » des données est l'amélioration des fonctionnalités des services cloud pour un enrichissement de l'expérience client. En ce qui concerne les limites à cette collecte de « masse », il est reporté que le client conserve la « maîtrise » sur ses données et peut ainsi se connecter à son compte Google pour gérer les données relatives à l'activité. Quand bien même le client conserverait la « maitrise » sur ses données, cela n'empêcherait pas le prestataire de services cloud à accéder aux données confidentielles du client pour les exploiter. Le champ de la collecte est tellement large (englobant tous types d'informations confidentielles) que le risque d'atteinte aux données personnelles des clients est accru. En effet, l'utilisateur ne dispose d'aucun moyen de vérifier ou de contrôler l'utilisation qui sera faite de ses données personnelles. Certaines dispositions du contrat [363] prévoient des prérogatives très larges au profit de Google, dont les limites ne semblent pas être perceptibles.

***143.*** En outre, l'intégration de cette disposition générique[364] dans un document qui ne requiert pas toujours un formalisme strict d'acceptation est critiquable au regard de l'impératif de protection des données à caractère personnel. Ce type de mention ne permet pas à la personne concernée de prendre connaissance des conséquences réelles concernant l'utilisation des données qui sont collectées. Dans d'autres situations, le consentement du client est susceptible d'être remis en cause lorsqu'il est donné de manière « tacite ». Le prestataire de services cloud estime que le consentement du client est donné dès lors qu'il utilise les services cloud (en l'occurrence, ici, un service cloud gratuit). Il s'agirait, donc, d'une application « d'office » de ces conditions. C'est dans cette configuration que nous pouvons évoquer l'idée d'*une forme de dépossession invisible des données à caractère personnel* de l'utilisateur (personne physique). En effet, en conférant une licence de collecte et de traitement des données avec un champ aussi large (sans formalisme strict d'acceptation), l'utilisateur risque de voir ses données exploitées à son insu. Ainsi, il en résulte de l'analyse de la politique de confidentialité, que certaines dispositions relatives aux

[361] Ibid.

[362] Ibid.

[363] V. *supra* n° 138.

[364] Ibid.

prérogatives du prestataire de services cloud peuvent prêter à discussion au regard de l'impératif de protection du droit fondamental à la protection des données à caractère personnel.

***144.*** Après avoir établi les critiques quant à l'intégration de la clause de collecte et de traitement des données dans le contrat de cloud computing, il est envisagé désormais d'étudier les déséquilibres contractuels causés par l'intégration de la clause de collecte et de traitement des données.

## B) L'existence d'un déséquilibre contractuel

***145.*** Par l'analyse des contrats de cloud computing, il apparaît que l'intégration de la clause de collecte et de traitement des données provoque des déséquilibres entre les droits et les obligations des parties et a une incidence directe sur la protection des données à caractère personnel des clients, personnes physiques.

***146.*** **Plan.** Ces déséquilibres contractuels se manifestent à travers la clause relative à l'exploitation des données (1) et les clauses limitatives ou élusives de responsabilités (2).

### 1) Par la clause d'exploitation des données

***147. Le risque d'exploitation des données à caractère personnel par les prestataires de services à l'insu du client***. La question qui intéresse la communauté des clients, personnes physiques, de services cloud est de savoir si le prestataire de services cède à d'autres entités les données à caractère personnel ainsi collectées auprès de ses clients. Sur ce point, certains prestataires de services cloud n'hésitent pas à affirmer dans leurs Conditions d'utilisation du service cloud qu'ils ne « vendent » pas les données à caractère personnel[365]. *A contrario*, il est légitime de penser que les données qui ne seraient pas « définies » dans les Conditions d'utilisation du service cloud comme étant des données à caractère personnel puissent faire l'objet d'un contrat de cession. Il est fondamental de définir précisément le champ des catégories de données à caractère personnel et des données à caractère non personnel. Puisque c'est à partir de ces définitions qu'il sera appliqué pour chacune de ces catégories, un régime spécifique d'exploitation (traitement) des données[366]. Certains contrats de cloud computing ne prévoient l'autorisation du client, personne physique, pour le traitement de certaines données, telles que

[365] Les règles de confidentialité et conditions d'utilisation des services de Google : https ://policies.Google.com/privacy.

[366] V. *supra* n° 10 et suivants.

les données rendues publiques. À titre illustratif dans le contrat iCloud d'Apple, il est mentionné que dès lors que l'utilisateur publie des données sur des parties accessibles au « public », Apple considère que l'utilisateur lui concède « une licence pour le monde entier à titre gratuit, non exclusive, d'utilisation, de distribution, de reproduction, de modification, d'adaptation, de publication, de traduction, d'exécution et de diffusion publique du Contenu sur le Service uniquement aux fins pour lesquelles ce contenu a été publié ou mis à disposition, sans aucune compensation ou obligation envers l'utilisateur »[367]. En d'autres termes, dès lors que l'utilisateur décide de rendre visible une donnée au public, Apple considère que le Client l'autorise à exploiter à titre gratuit ladite donnée. L'intégration de cette disposition semble contestable puisqu'elle permet d'accorder des prérogatives à Apple sur les données du client sans que le consentement de ce dernier soit exigé. En outre, la rédaction actuelle de cette disposition ne semble pas être exhaustive et ne permet d'éclairer le client, personne physique, quant au périmètre de la collecte et du traitement des données. Concernant cette donnée qui est rendue visible au public, il convient d'en déterminer sa nature aux fins d'identification du régime applicable. Peut-elle être considérée comme étant une donnée à caractère personnel, une donnée se rattachant à la vie privée de l'intéressé ou une donnée à caractère non personnel ? La jurisprudence a considéré concernant les données publiques (celles accessibles au public à partir des réseaux sociaux, des sites internet ou autres registres publics…) que « ce n'est pas parce que des données ont été diffusées, c'est-à-dire portées à la connaissance ou rendues accessibles à un nombre indéfini de personnes, qu'elles ne bénéficient plus d'une protection. En d'autres mots, il n'est pas question de dépouiller de toute protection des données dès lors qu'elles sont rendues publiques d'une quelconque façon, que ce soit notamment sur internet ou dans un journal »[368]. Il en résulte de cette jurisprudence que la donnée à caractère personnel ou la donnée rattachée à la vie privée de la personne continue de bénéficier d'une protection légale indépendamment de son accessibilité au public.

***148. L'indétermination de l'étendue du droit de collecte et de traitement des données dans le cadre de services cloud « gratuit »***. L'attraction massive des personnes physiques pour la technologie du cloud est provoquée, d'une part, par la gratuité, mais surtout par une offre de prestations de services cloud enrichie de nouvelles fonctionnalités de plus en plus innovantes et performantes techniquement. Les clients, personnes physiques, vont « délaisser » au prestataire de services cloud des informations qui se rattachent à la vie privée en contrepartie de la gratuité de ces services cloud et aux nombreux bénéfices qu'ils en retirent.

[367] Contrat i.cloud d'Apple : https ://www.apple.com/legal/internet-services/icloud/fr/terms.html.

[368] CJUE, 16 décembre 2008, affaire n° C-73/07, Tietosuojavaltuutettu c. Satakunnan markkinapörssi oy et Satamedia oy.

***149.*** Dans les contrats de cloud computing dit « gratuit », les dispositions relatives aux services cloud sont rédigées de manière très large de sorte qu'elles sont susceptibles de porter atteinte au droit à la protection des données à caractère et au droit à la vie privée. Très souvent, le prestataire de services cloud exige du client en contrepartie de l'utilisation gratuite du service cloud une autorisation de collecte et de traitement des données. Le client, personne physique souhaitant bénéficier de ce service cloud, va accepter d'accorder au prestataire cette licence de collecte et de traitement des données. Certes, cette pratique repose sur le principe de la volonté des parties et de la force obligatoire du contrat[369] et pourtant elle demeure critiquable au regard de la nécessité de préserver les droits et libertés fondamentaux. En l'espèce, les clients se voient contraints dans une certaine mesure d'abandonner une part de leur vie privée en échange d'un service technologique qui de nos jours devient de plus en plus indispensable.

***150.*** Dès lors qu'un service cloud est *gratuit*, le client, personne physique doit être vigilant et être informé des conséquences de l'utilisation des services cloud sur la protection de ses données et de son droit à la vie privée. Il est fréquent d'observer, dans les contrats cloud « *gratuit* », des clauses qui accordent une large autorisation de collecte et de traitement des données. A ce titre, le contrat cloud de Google dispose que « cette autorisation demeure pour toute la durée légale de protection de votre contenu, même si vous cessez d'utiliser nos Services »[370]. Pour éviter la censure de cette disposition, Google a tout de même prévu des limitations ; il est indiqué que « les droits que vous accordez dans le cadre de cette licence sont limités à l'exploitation, la promotion ou à l'amélioration de nos services, ou au développement de nouveaux services »[371]. Compte tenu de cette disposition, Google devrait utiliser ces droits tirés de la licence dans le strict cadre de l'exploitation, la promotion ou l'amélioration de ses services, ou au développement de nouveaux services.

***151.*** Malgré ces limitations contractuelles, il n'en reste pas moins que cette disposition générique est susceptible de porter atteinte au droit à la protection des données à caractère personnel et au droit à la vie privée. Le Prestataire de services cloud pourrait, ici, prévoir tout type d'usage des données sous la justification de développer et améliorer les services cloud. De plus, cette exploitation est difficilement mesurable en raison d'une appréciation des dispositions pouvant être très extensive. À ce titre, il est précisé dans les règles de confidentialité, que Google a le droit d'utiliser les données des personnes physiques stockées dans le cloud ; que les systèmes automatisés accèdent aux données des clients y compris les courriels afin d'analyser le contenu

[369] Article 1103 du code civil : « Les contrats légalement formés tiennent lieu de loi à ceux qui les ont faits ».

[370] Les conditions d'utilisation du service cloud de Google : https ://policies.Google.com/terms.

[371] Ibid.

qui pourtant relève de la confidentialité et de la vie privée des personnes[372]. Il est évident, ici, que le prestataire de services cloud exploite massivement les données de ses clients, personnes physiques. Concernant cette exploitation d'exploitation des données, la société Google justifie ces atteintes par la possibilité de faire bénéficier à ses clients de fonctionnalités plus performantes et pertinentes dans le cadre de l'utilisation de ses services cloud.

***152.*** En revanche, si les prestataires de services cloud décident de collecter et de traiter les données à caractère personnel des utilisateurs, ils sont tenus d'appliquer les dispositions du RGPD. Ces derniers ont, donc, l'obligation de mettre leurs politiques et conditions du service cloud en conformité avec la réglementation en vigueur en matière de protection des données. Ils doivent intégrer dans leurs processus et documents contractuels, les droits garantis par le RGPD et les droits fondamentaux par la Charte de l'Union européenne (2000/C364/01) ; en particulier le droit au respect à la vie privée[373] et familiale et le droit à la protection des données à caractère personnel[374]. En présence d'une clause de collecte et de traitement des données, le prestataire doit mentionner, dans le contrat, les droits à la protection des données garantis par le RGPD, tel que le droit d'exporter les données pour en faire une copie ou une sauvegarde (article 20), de supprimer le contenu des services et les informations du compte (article 17), d'exercer le droit d'accès (article 15), de demander une rectification (article 16), une restriction du traitement des données (article 18) ainsi que le droit de s'opposer au traitement des données (article 21). La mention de ces droits dans les Conditions d'utilisation est une obligation légale et ne peut pas avoir pour effet d'éluder les atteintes contractuelles au droit à la protection des données à caractère personnel et au droit à la vie privée.

***153.*** Après avoir étudié les déséquilibres contractuels par la clause relative l'exploitation des données, il est question de les étudier à travers les clauses limitatives ou élusives de responsabilités.

---

[372] Ibid.

[373] Article 7 de la Charte des droits fondamentaux de l'Union européenne (2000/ C364 /01) : respect de la vie privée et familiale : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications ». Les droits garantis à l'article 7 correspondent à ceux qui sont garantis par l'article 8 de la CEDH lequel dispose que « 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

[374] V. art. 8 de la Charte des droits fondamentaux de l'Union européenne (2000/ C364 /01).

**2) Par les clauses élusives et limitatives de responsabilités**

***154. La responsabilité du client pour la sécurité des données***. La question se pose de savoir qui est responsable de la sécurité des données dans les contrats de cloud computing. Il apparaît que le contrat de cloud computing désigne le client, personne physique, comme étant le responsable concernant la sécurité de ses données stockées dans le cloud computing. Cette désignation de « responsabilité » est expressément mentionnée dans le contrat « iCloud d'Apple » dans lequel il est précisé qu'il s'agit de la responsabilité de l'utilisateur, personne physique, de veiller à la sécurité et à la confidentialité des données du compte[375]. Cette mention permet à Apple de limiter (voire d'exclure) sa responsabilité en cas d'atteinte des données du client en raison, par exemple, d'une utilisation par un tiers du compte client. Il en résulte que les dispositions prévoyant une responsabilité à la charge de l'utilisateur peuvent soulever des interrogations quant à l'équilibre des droits et des obligations des parties au contrat.

***155.*** Est-ce que ces clauses, imposant au client, personne physique, une obligation de sécurité de ses données dans le cloud, sont caractéristiques d'un déséquilibre significatif entre les droits et les obligations des parties ; en particulier lorsque le contrat prévoit une autorisation de collecte et de traitement des données au profit du Prestataire ? Est-il légitime de faire supporter la charge de la sécurité des données uniquement sur le client alors même que le prestataire de services cloud bénéficie d'une autorisation de collecte et de traitement des données et donc dispose lui aussi d'un accès aux données ? Pour répondre à ces questions, il faudrait envisager précisément quelles sont les prérogatives de chacun sur les données stockées et en particulier identifier la personne ayant effectivement la « maîtrise » sur la donnée. La « maîtrise » est entendue, en matière de cloud computing, comme étant un pouvoir de décision et de direction concernant la gestion et l'utilisation des données. Il apparaît qu'en matière de cloud computing, c'est le client, utilisateur, qui conserve la « maîtrise » sur ses données. En conséquence, il semble légitime de lui imposer une obligation de sécurité sur ses données (notamment par la mise en place de « mots de passe » pour sécuriser l'accès à ses données dans le cloud). Il en résulte que le déséquilibre ne proviendrait pas de l'imputation de la responsabilité à la charge du client-personne physique quant à la sécurité de ses données, mais davantage dans l'intégration d'une clause de collecte et de traitement des données dans les contrats de cloud computing.

[375] V. Contrat icloud d'Apple : https ://www.apple.com/legal/privacy/fr-ca/. Également, s'agissant de la diffusion du contenu, il est rappelé que c'est « l'utilisateur » du service icloud qui en est responsable. A ce titre, il est mentionné qu'Apple ne peut en aucun cas être tenue pour responsable du contenu fourni par d'autres et n'a aucune obligation d'examiner ce « contenu ». En revanche, il est précisé que si le contenu s'avère contraire au contrat, Apple « peut examiner, déplacer, refuser, modifier ou supprimer à tout moment du Contenu, sans préavis et à son entière discrétion » : Contrat icloud d'Apple : https ://www.apple.com/legal/internet-services/icloud/fr/terms.html.

***156. Une obligation de moyens du prestataire de services cloud***. Très souvent, les contrats de cloud computing mentionnent que l'obligation dans la délivrance des services du prestataire n'est que de moyens et non de résultats. À titre illustratif, le prestataire de services Google indique dans ses Conditions d'utilisation que « l'offre de services est soumise à une obligation de moyens »,[376] et que « ni ses fournisseurs ou distributeurs, ne font aucune promesse spécifique concernant les Services. Par exemple, nous ne contractons aucun engagement concernant le contenu des Services, les fonctionnalités spécifiques disponibles par le biais des Services, leur fiabilité, leur disponibilité ou leur adéquation à vos besoins. Nous fournissons nos Services « en l'état »[377]. De ces mentions, il en résulte deux conséquences, d'une part, le prestataire limite sa responsabilité (ici obligation uniquement de moyens) et d'autre part, une limitation de garantie (réparation limitée en cas de manquement). Concernant la limitation de responsabilité et donc de garantie, il est spécifié « que dès lors la responsabilité de Google serait retenue l'indemnisation est limitée au montant que l'utilisateur à payer pour utiliser les services »[378]. Dans cette hypothèse, le client, personne physique, ne peut prétendre à une indemnisation supérieure au montant qu'il aura payé pour utiliser les services cloud. Cette limitation de garantie (indemnisation) est critiquable puisque cette indemnisation (laquelle est limitée au montant effectivement payé pour l'utilisation des services) serait insuffisante pour couvrir le préjudice issu d'une atteinte au droit à la protection des données à caractère personnel et au droit à la vie privée. Pour encadrer davantage cette limitation de garantie, les contrats de cloud computing précisent par une disposition spécifique que l'indemnisation ne peut porter que sur les dommages prévisibles. Certes, en matière de responsabilité contractuelle, l'indemnisation du « dommage prévisible » est la règle, mais les prestataires de services cloud vont intégrer dans leurs contrats cloud des clauses tellement limitatives, voire élusives, de responsabilités[379] qu'il sera difficile pour l'utilisateur (personne physique) d'obtenir un dédommagement de son préjudice. Par cette analyse des dispositions, il en résulte que la protection des données dans les contrats de cloud computing est « menacée » par cette ingénierie contractuelle.

***157. Une exclusion de responsabilité contestable.*** Dans certains contrats de cloud computing, il est observé l'insertion de clauses ayant pour objet d'exonérer le prestataire de services cloud de toute responsabilité. À titre illustratif, il est mentionné dans les Conditions d'utilisation de

[376] Les conditions d'utilisation du service cloud de Google : https ://policies.Google.com/terms.

[377] Ibid.

[378] Ibid.

[379] Sur ce point, il est affirmé le principe qu'Apple ne peut être tenue responsable envers l'utilisateur de « tout dommage direct, indirect, accidentel, particulier, immatériel ou exemplaire, y compris sans s'y limiter, les dommages pour perte de profits, de clientèle, d'utilisation, de données, de coûts d'acquisition de biens ou services de remplacement, ou toute autre perte intangible (…) » https ://www.apple.com/legal/internet-services/icloud/fr/terms.html . Ainsi par cette disposition contractuelle, Apple ne pourrait pas être tenue responsable en cas de pertes de données.

services cloud de Google, qu'elle ne soit pas responsable pour « les pertes de bénéfices, de revenus ou de données, ou les dommages et intérêts indirects, spéciaux, consécutifs, exemplaires ou punitifs »[380]. En l'espèce, il est expressément stipulé que même dans la situation d'une perte de données, aucune responsabilité ne peut être engagée à l'égard du prestataire de services cloud Google. De manière plus étendue et univoque, le contrat iCloud d'Apple mentionne qu'Apple ne peut être tenue responsable envers l'utilisateur de « tout dommage direct, indirect, accidentel, particulier, immatériel ou exemplaire, y compris sans s'y limiter, les dommages pour perte de profits, de clientèle, d'utilisation, de données, de coûts d'acquisition de biens ou services de remplacement, ou toute autre perte intangible (…) »[381]. Dans le même sens, Apple affirme s'exonérer de toute responsabilité en cas de « perte, altération, attaque, virus, interférence, piratage ou autre atteinte à la sécurité » et ajoute que « toute information téléchargée ou obtenue par le biais de l'utilisation du service est accessible à votre propre discrétion et à vos risques et périls, et vous serez l'unique responsable des dommages causés à votre appareil, ordinateur, ou de la perte des données résultant du téléchargement de telles informations »[382]. Ces dispositions énoncent expressément et sans équivoque l'exclusion de toute responsabilité du prestataire de services cloud (en l'occurrence Apple) concernant les dommages causés aux données stockées dans l'icloud. Cette mention est cohérente dès lors qu'on la rattache à une autre prévision contractuelle du même contrat, laquelle a pour objet de mettre une obligation de sécurité des données à la charge du client, personne physique. En effet, si le client est désigné comme étant le responsable quant à la sécurité des données stockées dans le cloud, il paraît normal que le prestataire de services cloud (ici Apple) exonère sa responsabilité en cas d'atteinte aux données par suite d'une défaillance du client quant à son obligation de sécurité des données.

***158.*** En outre, ces clauses limitatives ou élusives de responsabilité ont pour effet d'engendrer corrélativement une exclusion ou une limitation d'indemnisation au profit de l'utilisateur, personne physique et cette restriction est critiquable puisque affaiblisse la portée et l'effectivité du droit fondamental à la protection des données à caractère personnel. Il ne fait, donc, aucun doute que ces mentions telles que rédigées ont un impact direct sur la protection des données dans les contrats de cloud computing puisqu'elles ont pour incidence de limiter voire d'exclure une indemnisation au profit du client, personne physique.

[380] Les conditions d'utilisation du service cloud de Google : https ://policies.Google.com/terms.

[381] Contrat i.cloud d'Apple : https ://www.apple.com/legal/internet-services/icloud/fr/terms.html.

[382] Ibid.

***159. La remise en cause des clauses « déséquilibrées ».*** Malgré l'existence de ces clauses limitatives ou élusives de responsabilité dans le contrat de cloud computing, le client, personne physique, a toujours la possibilité de les remettre en cause dans le cadre d'une action judiciaire si elles ont pour objet de créer un déséquilibre significatif entre les droits et les obligations des parties au contrat. Lorsqu'il existe un déséquilibre significatif dans un contrat de cloud computing conclu entre une prestataire de services cloud et un consommateur (personne physique qui n'agit pas en qualité de professionnel), alors ce sont les règles du droit spécial qui s'appliquent et en particulier L. 212-1 du code de la consommation modifié par l'ordonnance du 14 mars 2016. En droit de la consommation, le déséquilibre significatif est appréhendé par la constatation de clauses abusives contenues dans un contrat ou un contrat lié et qui ne porte « ni sur la définition de l'objet principal du contrat ni sur l'adéquation du prix ou de la rémunération au bien vendu ou au service offert » à la condition que ces clauses « soient rédigées de façon claire et compréhensible ». Tel que rappelé par la doctrine, le système de protection mis en œuvre par la directive sur les clauses abusives est lié à la situation d'infériorité du consommateur à l'égard du professionnel, « en ce qui concerne tant le pouvoir de négociation que le niveau d'information », situation qui conduit le consommateur à adhérer aux conditions rédigées préalablement par le professionnel, sans pouvoir exercer une influence sur le contenu de celles-ci. À l'instar du droit commun des contrats, la sanction est, également « le réputé non écrit de ces clauses conformément à l'article L.241-1 du code de la consommation. Sur le fondement de l'article L.212-1 du code de la consommation, les juges ont systématiquement déclaré comme abusives certaines clauses du contrat qui créent un déséquilibre contractuel au détriment de l'utilisateur d'un service cloud, telles que les clauses relatives à loi applicable et l'attribution de compétence. En présence de telles clauses abusives, le client peut demander aux juges de considérer ces clauses limitatives ou élusives de responsabilité comme étant « réputées non écrites »[383].

***160.*** Il est rappelé, ici, que pour prétendre à la sanction du « réputé non écrit », ces clauses limitatives et/ou élusives de responsabilité doivent être considérées par les juges comme étant des clauses « abusives », c'est-à-dire qu'elles sont de nature à créer un déséquilibre significatif dans les droits et les obligations des parties[384]. À titre illustratif, le tribunal judiciaire de Paris a

[383] V. art. L241-1 du code de la consommation, crée par l'ordonnance n°2016-301 du 14 mars 2016, « Les clauses abusives sont réputées non écrites. Le contrat reste applicable dans toutes ses dispositions autres que celles jugées abusives s'il peut subsister sans ces clauses. Les dispositions du présent article sont d'ordre public ».

[384] V. art. L212-1 du code de la consommation, modifié par l'ordonnance n°2016131 du 10 février 2016- art.2, : « 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. Sans préjudice des règles d'interprétation prévues aux articles 1188, 1189, 1191 et 1192 du code civil, le caractère abusif d'une clause s'apprécie en se référant, au moment de la conclusion du contrat, à toutes les circonstances qui entourent sa conclusion, de même qu'à toutes les autres clauses du contrat. Il s'apprécie également au regard de celles contenues dans un autre contrat lorsque les deux contrats sont juridiquement liés dans leur conclusion ou leur exécution ».

décidé de déclarer abusives les clauses contenues dans les conditions d'utilisation du service Apple music dans les versions v4 (septembre 2018) et v5 (mai 2019) lesquelles étaient relatives aux exclusions de garanties, aux limitations et exonérations de responsabilité, aux envois de contenu au service Apple music, à la disponibilité du contenu, à la résiliation, à la suspension des services, à l'utilisation de contenu, aux modifications du contrat. À titre de sanction, le tribunal a déclaré ces clauses comme réputées non écrites[385]. Il est envisagé de développer cette jurisprudence pour obtenir des clés de compréhension quant à l'analyse du caractère déséquilibré des clauses insérées dans un contrat de cloud computing.

***161.*** En l'espèce, c'est l'association UFC QUE CHOISIR qui a introduit un recours contre la société ADI (Apple Distribution International), société de droit irlandais devant le tribunal de grande instance de Paris, devenu tribunal judiciaire de Paris, aux fins de faire constater le caractère abusif et/ou illicite des clauses des "Conditions d'Utilisation" de la société ADI, dans la version du 30 juin 2015, dénommée par les parties Conditions générales VI, de mars 2016 "Conditions générales V2", du 13 septembre 2016 "Conditions générales V3", du 17 septembre 2018 "Conditions générales V4" et du 13 mai 2019 "Conditions générales V5", le caractère illicite des clauses des "Politiques de confidentialité", dont le document intitulé "Engagement de Confidentialité " dans les versions des 22 mai 2018, 09 mai 2019, le document intitulé "Apple Music et confidentialité" du 18 septembre 2018 ainsi que le document intitulé "À propos du lecteur Web Apple Music et de la confidentialité", les faire supprimer et/ou modifier, de les faire réputées non écrites et de réparer le préjudice causé à l'intérêt collectif des consommateurs. Spécifiquement, l'association demande au tribunal de déclarer abusives et illicites l'ensemble des clauses des Conditions d'Utilisation relatives aux exclusions de garanties, aux limitations de responsabilité, à l'envoi de contenu au service Apple music, à la disponibilité du contenu, à la résiliation et suspension des services, à l'utilisation de contenu, ainsi que de déclarer abusive la Politique de Confidentialité d'ADI dans son ensemble comme créant un déséquilibre significatif entre les droits et obligations d'ADI et des consommateurs, et la déclarer illicite comme contraire, au principe de transparence prévu par le RGPD et le Code de la consommation. Concernant le caractère abusif et/ou illicite, il est mis en cause l'absence de clarté et de compréhensibilité de certaines clauses au regard de l'article L.211-1 du code de la consommation. L'association met en cause « l'emploi de termes vagues et d'expressions imprécises ne permettant pas à l'utilisateur/consommateur de connaître l'engagement de la société ADI sur la qualité du service qu'il propose (..) et que le régime de responsabilité (...) ne peut se comprendre qu'au prix d'une lecture combinant la première et la dernière phrase de la clause et d'un raisonnement qui n'est pas accessible à l'ensemble des consommateurs ». En

[385] Tribunal judiciaire de Paris, 9 juin 2020, affaire n° 16/09799.

transférant la responsabilité de la société ADI sur l'utilisateur, cette clause est considérée comme créant, alors, un déséquilibre significatif entre les droits et obligations de l'utilisateur et d'ADI. En outre, l'association considère que les clauses mises en cause sont illicites au regard des articles L.211-1 du code de la consommation, des articles 4, 12, 13, 14 du RGPD et sont abusives au regard des articles L.212-1 et R.212-1 4° du code de la consommation et demande la sanction du réputé non écrit. Le tribunal judiciaire de Paris décide d'accéder à la demande de l'association en déclarant réputées non-écrites, en raison de leur caractère illicite ou abusif, les clauses relatives aux exclusions de garanties, aux limitations de responsabilité, la clause d'exonération de responsabilité, les clauses "envoi de contenu au service Apple music" et "vos envois sur nos services", la clause "disponibilité du contenu", la clause "résiliation", la clause "résiliation et suspension des services", la clause "utilisation de contenu", les clauses "modifications" "modifications du contrat" et les clauses figurant dans les conditions d'utilisation du service Apple music dans les versions v4 (septembre 2018) et v5 (mai 2019). Également, le tribunal condamne la société ADI à payer au profit de l'association UFC - QUE CHOISIR la somme de 20.000 euros à titre de dommages-intérêts en réparation du préjudice occasionné à l'intérêt collectif des consommateurs.

***162.*** Pour atteindre un certain équilibre contractuel entre les droits et les obligations des parties au contrat, le prestataire de services cloud devra s'assurer que le contrat ne contient pas de clauses au détriment du client et si oui il devra prévoir une modification du contrat soit par la voie de l'avenant soit par l'intégration de conditions particulières. Il faudra accorder une importance particulière aux clauses relatives aux obligations des parties, à la responsabilité, la durée et la résiliation. Il apparaît fréquemment que le prestataire de services de cloud computing met à la charge du client un certain nombre de responsabilités concernant les activités opérées depuis le compte « cloud »[386] et le contenu des données stockées dans le cloud[387]. Ces clauses de responsabilités sont rédigées de manière très large afin de laisser peu de place à l'engagement de la responsabilité du prestataire de services cloud. À titre d'exemple, il est reproduit, ci-dessous, une clause issue du contrat cloud d'Amazon web Services (AWS) stipulant que « les offres de services sont fournies "telles quelles", qu'elle ne formule aucune déclaration, ne donne aucune garantie quelconque, qu'elle soit explicite ou implicite » et exclut sa responsabilité concernant « tout dommage direct, indirect, fortuit, spécial, consécutif ou exemplaire (y compris

[386] Concernant les comptes, il est spécifié à l'égard de son client que « vous êtes responsable de toutes les activités ayant lieu dans le cadre de votre compte, que vous les ayez autorisées ou qu'elles soient menées par vous, vos salariés ou un tiers (y compris vos sous-traitants, agents ou Utilisateurs Finaux) et (b) nous, ainsi que nos sociétés affiliées, déclinons, toute responsabilité concernant tout accès non autorisé à votre compte » https ://d1.awsstatic.com/legal/aws-customer-agreement/AWS_Customer_Agreement-FR_(2019-04-30).pdf.

[387] S'agissant du contenu, il est indiqué que le client est « seul responsable du développement, du contenu, du fonctionnement, de l'entretien et de l'utilisation de Votre Contenu » https ://d1.awsstatic.com/legal/aws-customer-agreement/AWS_Customer_Agreement-FR_(2019-04-30).pdf.

tous dommages de perte de profits, de revenus, de clientèle, d'opportunités, de notoriété, d'utilisation ou de données) » et n'assure aucun dédommagement, remboursement ou dommages et intérêts survenant en raison de (..) (d) tout accès non autorisé à votre contenu ou à d'autres données, leurs altération, suppression, destruction, dommage, perte ou défaut de stockage »[388]. Cette clause a pour effet d'éluder la responsabilité du prestataire dans de nombreux cas. Elle est rédigée de manière très large afin de couvrir dans son champ le plus possible de situations rencontrées en pratique. Bien que consenties et approuvées par les parties, ces clauses, dès lors, qu'elles auront pour effet de créer un déséquilibre significatif pourront être remises en cause dans le cadre d'une procédure judiciaire.

***163.*** Pour prévenir ce type d'action, les prestataires de services cloud intègrent dans leurs conditions d'utilisation de services cloud, une disposition générique mentionnant l'application au profit du client, personne physique, des droits issus de la réglementation en vigueur relative aux droits du consommateur. À titre illustratif, Google précise dans ses Conditions d'utilisation du service cloud que : « si vous utilisez les services pour un usage personnel, aucune disposition des présentes Conditions d'Utilisation ou des conditions d'utilisation supplémentaires ne limite les droits légaux du consommateur auxquels aucun contrat ne peut déroger »[389]. Également, il est mentionné le rappel des droits des utilisateurs garantis par le RGPD plus ou moins exhaustif en fonction du type du contrat cloud[390] afin d'échapper à toute sanction.

***164. La responsabilité de plein droit dans le cadre d'un contrat à distance***. Dans le cadre d'un contrat de cloud computing conclu à distance entre un professionnel et un consommateur[391], il existe une responsabilité de plein droit concernant le manquement aux obligations d'informations conformément à L. 221-15 du code de la consommation,[392] lequel a été crée par

[388] Clause élusive de responsabilité dans le Contrat cloud d'Amazon Web Services : https ://d1.awsstatic.com/legal/aws-customer-agreement/AWS_Customer_Agreement-FR_(2019-04-30).pdf.

[389] Les conditions d'utilisation du service cloud de Google : https ://policies.Google.com/terms.

[390] Illustration de processus mis en place par Apple pour se conformer à la règlementation protectrice des consommateurs et en particulier ici du RGPD : La politique de confidentialité d'Apple stipule « qu'Apple fournit à ses utilisateurs l'accès aux informations à caractère personnel, avec la possibilité de faire une copie afin d'être en mesure par la suite de demander une correction ou une suppression ». Également, il est mis en place un processus pour répondre aux questions relatives à la confidentialité des données. Ainsi, « l'utilisateur peut contacter le responsable de la protection des données et lui adresser une demande puis une réponse est en principe fournie dans un délai de sept (7) jours. Également, l'utilisateur conserve la possibilité de « déposer une plainte en tout temps auprès du responsable de la réglementation de votre région si vous n'êtes pas satisfait d'une réponse que vous avez obtenue de notre part » : Contrat icloud d'Apple : https ://www.apple.com/legal/privacy/fr-ca/.

[391] Article liminaire du code de la consommateur : le consommateur est défini comme étant « toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale ».

[392] Article L.221-15 du code de la consommation : « Le professionnel est responsable de plein droit à l'égard du consommateur de la bonne exécution des obligations résultant du contrat conclu à distance, que ces obligations soient exécutées par le professionnel qui a conclu ce contrat ou par d'autres prestataires de services, sans préjudice de son droit de recours contre ceux-ci. Toutefois, il peut s'exonérer de tout ou partie de sa responsabilité en apportant la preuve que l'inexécution ou la mauvaise exécution du contrat est imputable soit au consommateur, soit au fait, imprévisible et insurmontable, d'un tiers au contrat, soit à un cas de force majeure ».

l'ordonnance du 14 mars 2016[393]. Le régime de responsabilité est prévu à l'article 15 de la LCEN[394] du 2 juin 2004, est rappelé à l'article L. 221-15 du code de la consommation[395]. À titre d'exemple, il est stipulé dans les conditions d'utilisation du contrat i-tunes d'Apple que « iTunes, ses dirigeants (...) ne pourront en aucun cas être tenus pour responsables de perte ou dommage causé par iTunes, ses salariés ou agents (..) lorsqu'ils auront causé un dommage, lorsqu'ils observent une "obligation légale de précaution" , ou lorsque le dommage ne (...) constitue pas une conséquence raisonnablement prévisible" (lorsque) l'aggravation de cette perte ou ce dommage résulte d'un manquement de (l'utilisateur) ou lorsque la "perte ou (le) dommage résulte de la décision prise par iTunes (...) de supprimer ou de refuser de traiter une information ou un contenu, d'avertir (l'utilisateur), de suspendre ou de résilier (son) accès au Service Apple Music ou de prendre toute autre mesure. »[396]. Or, cette exclusion de responsabilité est critiquable au regard de la responsabilité de plein droit instituée par l'article 15 de la LCEN repris à l'article L. 221-15 du code de la consommation. Cette clause pourra être remise en cause dans le cadre d'une action judiciaire.

***165.*** Il en résulte de l'analyse de ces dispositions contractuelles qu'il revient au client, personne physique, de considérer avec attention les clauses relatives à la collecte et au traitement des données ainsi que celles établissant les droits et les obligations des parties afin de minimiser au mieux l'atteinte susceptible d'être portée à la protection de ses données à caractère personnel.

[393] Ordonnance n° 2016-301 du 14 mars 2016 relative à la partie législative du code de la consommation, JORF n°0064 du 16 mars 2016.

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

[395] Le professionnel est responsable de plein droit à l'égard du consommateur de la bonne exécution des obligations résultant du contrat conclu à distance, que ces obligations soient exécutées par le professionnel qui a conclu ce contrat ou par d'autres prestataires de services, sans préjudice de son droit de recours contre ceux-ci. Toutefois, il peut s'exonérer de tout ou partie de sa responsabilité en apportant la preuve que l'inexécution ou la mauvaise exécution du contrat est imputable soit au consommateur, soit au fait, imprévisible et insurmontable, d'un tiers au contrat, soit à un cas de force majeure.

[396] Conditions d'utilisation des services iTunes d'apple, clause relative aux exclusions de garanties et des limitations de responsabilité dans les versions v2, v3, v4 et v5 du 30 juin 2015.

# Conclusion du chapitre 1

***166. L'absence de règles spécifiques à la technologie du cloud et l'application contestable de la réglementation relative à la protection des données à caractère personnel.*** Dès lors que le contrat de cloud computing intègre une clause de collecte et de traitement des données au profit du prestataire de services cloud, la réglementation relative à la protection des données à caractère personnel à vocation à s'appliquer et en particulier celle du RGPD. On s'aperçoit très rapidement que cet instrument qu'est le RGPD se limite à la protection des données à caractère personnel et n'est pas spécifique à une protection des données dans les contrats de cloud computing. Si nous partons du postulat qu'un contrat de cloud computing ne devrait pas, en principe, contenir une clause autorisant la collecte et le traitement des données alors on aboutirait à l'exclusion de l'application du RGPD. Il a, donc, été proposé d'envisager un régime spécifique instaurant un principe d'interdiction de la collecte et du traitement des données dans le cadre de l'exécution d'un contrat de cloud computing. Cette proposition ne peut être retenue en raison des intérêts découlant de la généralisation de la collecte et de l'exploitation des données au profit des acteurs publics (états, organisations, administrations…) et privés (entreprises).

***167. Les critiques de l'intégration d'une clause de collecte et de traitement des données dans les contrats de cloud computing.*** L'application du RGPD au contrat de cloud computing est, certes, justifiée par l'existence d'une clause de collecte et de traitement des données, mais l'intégration de cette clause dans les contrats de cloud computing est contestable. Ces critiques sont fondées, tout d'abord, sur les spécificités du contrat de cloud computing et en particulier son objet, sa nature et son champ d'application. En raison de la perte de maîtrise du client, personne physique, sur l'utilisation de ses données personnelles, il a été évoqué l'idée « d'une forme de dépossession invisible de ses données personnelles ». Ensuite, il est constaté des déséquilibres entre les droits et les obligations et en particulier au niveau des clauses relatives à l'exploitation des données et aux limitations de responsabilité. Il en résulte que l'intégration dans le contrat cloud d'une autorisation de collecte et de traitement des données par le prestataire a pour conséquence d'affaiblir la protection des données à caractère personnel.

***168.*** Après avoir étudié l'application imparfaite du régime général de la protection des données à caractère personnel, il est envisagé d'étudier, à présent, l'application imparfaite du régime du transfert des données à caractère personnel au contrat de cloud computing.

# Chapitre 2 : L'application imparfaite du régime du transfert des données à caractère personnel au contrat de cloud computing

***169. L'impact de la localisation des serveurs et de l'identité du prestataire***. Avec le cloud computing, l'infrastructure informatique est très souvent délocalisée à l'extérieur de l'entreprise dans des serveurs situés dans des « datacenters » dont on ignore précisément leurs emplacements. Les services de cloud computing transnationaux suscitent des questions juridiquement complexes. Il y a donc une incertitude juridique qui est due par la délocalisation du stockage des données dans des serveurs situés hors des frontières du territoire national voire de l'Union européenne. Dans un contexte de mondialisation se pose la question de l'impact de la localisation de ces serveurs et de la nationalité de l'entreprise prestataire des services cloud sur la protection des données. La localisation des serveurs et la nationalité de l'entreprise prestataire de services cloud sont deux indicateurs permettant d'identifier, notamment pour les États-Unis, la réglementation applicable et les éventuels risques sur la protection des données.

***170. L'établissement d'une réglementation transnationale***. Pour préserver l'équilibre entre « la protection des données » et « la liberté de commerce et de l'industrie »[397], les États au sein de l'Union européenne ont établi, au travers de concessions réciproques, une réglementation commune pour la protection des données à caractère personnel (RGPD). Pour des raisons de sécurité juridique et d'intelligibilité des normes, il devenait primordial d'établir une réglementation transnationale d'application directe relative à la protection des données à caractère personnel[398]. Ce texte permet par son effet direct dans l'ordre juridique interne[399]

[397] La liberté de commerce et de l'industrie a été instituée par l'article 7 de la loi des 2 et 17 mars 1791 dite « décret d'Allarde » puis confirmée par la loi des 14 et 17 juin 1791 dite « Le Chapelier ». La liberté de commerce et de l'industrie recouvre la liberté d'entreprendre, la liberté d'exploitation, la liberté de la concurrence et découle de l'article 4 de la Déclaration des droits de l'homme et du citoyen énonçant que « La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui ». Par la suite, le Conseil Constitutionnel a, dans sa décision n° 81-132 DC, consacré la valeur constitutionnelle de la liberté d'entreprendre : Décision n° 81-132 DC, 16 janvier 1982, Loi de nationalisation, cons. 16, Rec. Cons. const. 18 ; AJDA 1982. 202.

[398] Le RGPD est un règlement européen et les règlements européens disposent toujours d'un effet direct en application de l'article 288 du Traité sur le Fonctionnement de l'Union européenne (TFUE), lequel précise en effet que les règlements sont directement applicables dans les pays de l'Union européenne. L'effet direct du droit européen a été consacré par la Cour de justice de l'Union européenne dans l'arrêt Van Gend en Loos du 5 février 1963 (CJUE 5 février 1963, affaire Van Gend en Loos, concernant le principe de l'effet direct des règlements européens). Dans cet arrêt, la Cour énonce que le droit européen engendre non seulement des obligations pour les pays de l'UE, mais également des droits pour les particuliers. Les particuliers peuvent, ainsi, se prévaloir de ces droits et invoquer directement des normes européennes devant les juridictions nationales et européennes. Il n'est alors pas nécessaire que le pays de l'Union européenne reprenne la norme européenne concernée dans son ordre juridique interne. Puis, la Cour de justice précise dans l'arrêt Politi du 14 décembre 1971 qu'il s'agit « d'un effet direct complet » (CJUE 14 décembre 1971, affaire Politi, apportant des précisions concernant le principe de l'effet direct des règlements européens). Ainsi, le RGPD dispose de l'effet direct et donc est applicable dans l'ordre juridique interne des pays membres sans qu'il soit nécessaire de passer par une loi de transposition nationale.

[399] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM%3Al1145.

d'uniformiser, au sein de l'Union européenne, les règles relatives à la protection des données à caractère personnel.

***171. La question de l'effectivité de la réglementation européenne pour la protection des données dans un contexte international***. La question est de savoir si les règles du RGPD relatives au transfert des données permettent d'assurer une protection des données à caractère personnel dans le cadre d'un contrat de cloud computing exécuté dans un contexte international. Au niveau de l'Union européenne, le texte applicable en matière de transfert de données à caractère personnel est celui du RGPD. Lors de l'établissement de ce texte, il a été fait le choix d'une conception très large des conditions d'application de cette réglementation afin de couvrir le plus possible les situations. Il est intéressant d'analyser comment le droit appréhende la question du transfert des données à caractère personnel. Il apparaît que cette réglementation distingue le transfert des données au sein de l'Union européenne et hors de l'Union européenne.

***172. L'identification des règles d'un transfert de données au sein de l'Union européenne.*** Au sein de l'Union européenne, le principe affirmé est celui de la libre circulation des données[400]. Dans le cadre d'une appréciation de la préservation des droits fondamentaux, certains auteurs ont critiqué la notion de libre circulation des données. Tel que le Professeur Benyekhlef l'avait déjà souligné dès 1992[401], la Professeure Benabou considère que « la référence continue au principe de la libre circulation de l'information, en ce qui concerne le secteur des transmissions de données personnelles, relève d'une erreur d'appréciation initiale, pour ne pas dire d'une imposture [...]. Là encore, les formidables enjeux économiques, dont les technologies de la communication électronique sont porteuses, sont à l'origine, croyons-nous, de cette extension, inacceptable au strict plan juridique, du principe de la libre circulation de l'information. La libre circulation est alors mise de l'avant, non pas pour assurer le respect des droits fondamentaux, mais bien plutôt pour conforter des intérêts commerciaux. La libre circulation de l'information se confond, dès lors, avec le libre-échange »[402]. Il s'agirait d'admettre que l'établissement d'un cadre européen de circulation des données serait non pas au service de la protection des données, mais servirait les intérêts économiques des acteurs privés (les entreprises) et publics (les États). Le principe de circulation des données a, également, été élargi aux données à caractère non personnel par le RDNP[403]. Avec l'adoption du RDNP et du RGPD, il s'agirait

[400] Article 1er du RGPD : « la libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ».

[401] Benyekhlef K., La protection de la vie privée dans les échanges internationaux d'informations, thèse, Thémis – Université de Montréal, 1992, p. 297.

[402] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279.

[403] Règlement (UE) numéro 2018/1807 du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne applicable depuis le 19 avril 2019. Ce texte a pour objet d'établir les règles en matière de transfert de données à caractère non personnel (celles qui ne concernent pas « une personne physique identifiée ou identifiable » et

ainsi de la création dans les textes européens d'une « cinquième liberté de circulation » applicables aux données[404]. Il en résulte qu'après la liberté de circulation des capitaux, des biens, des services et des personnes, voici donc celle des données. Ce principe d'une liberté de circulation des données est renforcé par le considérant 13 du RGPD qui énonce que « pour que le marché intérieur fonctionne correctement, il est nécessaire que la libre circulation des données à caractère personnel au sein de l'Union ne soit ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. (…) »[405]. Ce principe de libre circulation des données n'est pas nouveau ; le considérant 3 de la Directive européenne de 1995[406] l'affirmait déjà[407]. Cette affirmation de principe énoncée dans la Directive de 1995 témoigne de la préoccupation, qui existait déjà à cette époque, d'établir un équilibre entre la libre circulation des données à caractère personnel au sein de l'Union européenne et la protection des données à caractère personnel. Par ailleurs, l'Union européenne souhaitait que les règles relatives à la protection des données à caractère personnel soient uniformisées au sein de l'Union européenne. Le RGPD a vocation à uniformiser les règles « du niveau de protection » des données à caractère personnel entre les États membres de l'Union européenne. C'est dans ce sens que le considérant 13 du RGPD établit « qu'afin d'assurer un niveau cohérent de protection des personnes physiques dans l'ensemble de l'Union, et d'éviter que des divergences n'entravent la libre circulation des données à caractère personnel au sein du marché intérieur, un règlement est nécessaire pour garantir la sécurité juridique et la transparence aux opérateurs économiques (…) ». Cette liberté de circulation des données est conditionnée au respect des principes découlant du RGPD que sont la licéité, la loyauté, la transparence, la limitation des finalités, la minimisation des données, l'exactitude, la limitation de la conservation, l'intégrité et la confidentialité des données[408]. Il est possible, de considérer que lorsque les données à caractère personnel objet d'un contrat de cloud computing sont transférées au sein de l'Union européenne celles-ci

---

celles qui « étaient initialement des données à caractère personnel, mais qui ont ensuite été rendues anonymes ») et le principe consacré est la libre circulation des données au sein de l'Union européenne.

[404] Corazza Bildt A-M., députée au Parlement européen, rapporteure, Avis du Comité économique et social européen sur la « Communication de la Commission au Parlement européen et au Conseil — Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne », publié au Journal officiel de l'Union européenne, le 15 janvier 2020.

[405] Considérant 13 du RGPD.

[406] Considérant 3 de la Directive 95/46/CE : « considérant que l'établissement et le fonctionnement du marché intérieur dans lequel, conformément à l'article 7 A du traité, la libre circulation des marchandises, des personnes, des services et des capitaux est assurée, nécessitent non seulement que des données à caractère personnel puissent circuler librement d'un État membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardés ».

[407] Considérant 3 de la Directive 95/46/CE : « l'établissement et le fonctionnement du marché intérieur (..) nécessitent non seulement que des données à caractère personnel puissent circuler librement d'un État membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardés ».

[408] V. art. 5 du RGPD qui définit les principes relatifs au traitement des données à caractère personnel.

bénéficient d'une protection dans la mesure où elles jouissent des mêmes garanties offertes par le RGPD. En revanche, l'inquiétude est maintenue concernant le transfert des données à caractère personnel hors de l'Union européenne dans le cadre de l'exécution d'un contrat de cloud computing.

***173.*** **Plan.** Il est procédé, en l'espèce, à l'étude du cadre réglementaire européen pour le transfert des données hors de l'Union européenne (Section 1) et à l'analyse critique de ce cadre au regard de l'impératif de protection des données dans les contrats de cloud computing (Section 2).

## Section 1 : L'identification du cadre légal du transfert des données hors de l'Union européenne

***174.*** L'Union européenne a établi un cadre légal uniforme concernant la protection des données personnelles. Au sein de l'Union européenne, les personnes physiques bénéficient du même régime concernant la protection de leurs données à caractère personnel. C'est en raison de l'uniformisation de ces règles de protection des données que le RGPD acte le principe de libre circulation des données au sein de l'Union européenne. En revanche, le transfert hors de l'Union européenne est encadré par des règles spécifiques. Cette partie envisage, alors, d'étudier le cadre légal pour autoriser le transfert de données à caractère personnel de l'Union européenne vers des pays tiers.

***175.*** **Plan.** Il est proposé d'étudier le cadre légal européen (A) et américain (B) en matière de transfert de données à caractère personnel dans le cadre de l'exécution d'un contrat de cloud computing.

### A) Les règles européennes du transfert de données à caractère personnel

***176.*** Afin d'appréhender le cadre légal européen en matière de transfert de données hors de l'Union européenne dans le cadre de l'exécution d'un contrat de cloud computing, il est nécessaire d'envisager les principes applicables au transfert et les règles relatives à l'extraterritroialité.

***177.*** **Plan.** Il est envisagé d'étudier les principes du transfert des données hors de l'Union européenne (1) et l'extraterritorialité en matière de transfert de données à l'international.

**1) Les règles du transfert de données de l'Union européenne à destination de pays tiers**

***178. Un cadre légal propice au transfert international.*** Le parlement européen et le Conseil de l'Union européenne ont affirmé dans le RGPD que les flux de données à caractère personnel à destination et en provenance de pays en dehors de l'Union et d'organisations internationales sont nécessaires au développement du commerce international et de la Coopération internationale. Le transfert des données hors des frontières n'est pas interdit et est bien perçu puisqu'il contribuerait au développement de l'économie. Sur ce point, il est affirmé que « la libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel »[409]. Cette disposition semble, tel qu'affirmé par la Professeure Benabou, établir « une hiérarchie entre les deux objectifs qui fait prévaloir la liberté de circulation sur la protection »[410].

***179.*** Pour qualifier un transfert de données hors de l'Union, le CEPD a détaillé trois critères cumulatifs dans son projet de lignes directrices[411] relatif à l'articulation entre l'article 3[412] et le chapitre V[413] du RGPD. Il est spécifié que « premièrement, le responsable du traitement ou le sous-traitant doit être soumis au RGPD pour le traitement donné. Cela signifie que l'un des critères de l'article 3 du RGPD (localisation de l'établissement ou des personnes concernées par le traitement) s'applique de sorte que le responsable ou le sous-traitant entre dans le champ d'application territorial du RGPD ; deuxièmement, le responsable ou le sous-traitant exportateur des données doit divulguer par transmission ou rendre les données accessibles par tout autre moyen à un autre responsable du traitement ou un sous-traitant importateur. (..). Le CEPD insiste, en l'espèce, sur le fait que, pour que ce second critère soit rempli, il faut que les données soient transmises ou rendues accessibles à un importateur différent de l'exportateur ; troisièmement, l'importateur des données doit se trouver dans un pays tiers ou être une organisation internationale, indépendamment du fait que cet importateur soit ou non soumis au RGPD en ce qui concerne le traitement donné, conformément à l'article 3 du RGPD »[414]. L'établissement de ces critères par le CEDP permet d'éclairer au mieux les parties concernées

[409] V. art. 1er paragraphe 3 du RGPD.

[410] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279.

[411] Lignes directrices n° 05/2021 du CEPD, 18 nov. 2021 concernant l'articulation entre l'article 3 et le chapitre V du RGPD.

[412] L'article 3 du RGPD détermine champ d'application territorial du RGPD.

[413] Le chapitre V du RGPD est relatif aux modalités de mise en œuvre en cas de transferts de données hors de l'Union.

[414] Eynard J. et Monteil M., Le CEPD apporte des précisions sur la notion de transfert international de données, Dalloz actualité 1 décembre 2021.

concernant les situations de transfert de données hors de l'Union européenne. Dès lors qu'est constatée l'existence d'un transfert de données hors de l'Union européenne, il faut se référer au chapitre 5 du RGPD qui traite des modalités à mettre en œuvre concernant ce type de transfert de données.

***180. Le principe général en matière de transfert de données hors de l'Union européenne***. Le principe général concernant le transfert des données vers des pays tiers ou à des organisations internationales est énoncé à l'article 44 du RGPD dont le contenu est reproduit ci-après : « Un transfert vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions définies dans le présent chapitre sont respectées, par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale. Toutes les dispositions du présent chapitre sont appliquées de manière que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis »[415]. Cette disposition expose expressément l'exigence de garantir un niveau de protection des données lors d'un transfert de données hors de l'Union européenne. Cette obligation pèse sur le responsable du traitement ainsi que sur le sous-traitant et vise non seulement le premier transfert hors de l'Union européenne, mais également les transferts ultérieurs. Cet article permet d'établir le cadre dans lequel un transfert hors de l'Union européenne peut avoir lieu.

***181. L'exigence de garantir un niveau de protection adéquat des données.*** Le principe est l'exigence de garantir un niveau de protection adéquat des données lors d'un transfert de données hors de l'Union européenne. Cela signifie *a contrario* qu'un transfert hors de l'Union européenne ne peut avoir lieu, si les droits dont bénéficient les personnes physiques pour la protection de leurs données à caractère personnel ne peuvent pas être garantis. En définitive, ce niveau de protection ne doit pas être compromis lors d'un transfert hors de l'Union européenne. Il est, à rappeler que cette exigence n'est pas nouvelle et figurait déjà dans des textes avant l'entrée en vigueur du RGPD. Plusieurs textes posaient les conditions dans lesquelles un transfert de données à caractère personnel pouvait avoir lieu hors de l'Union européenne. La loi du 6 janvier 1978 modifiée (loi informatique et liberté) établit le principe que les données à caractère personnel ne peuvent être transférées en dehors de l'Union européenne que si le pays

[415] Article 44 du RGPD.

en question offre un « niveau de protection adéquat »[416]. La Directive européenne du 24 octobre 1995, afin de veiller au niveau de protection lors du transfert, exigeait avant tout transfert de données, une déclaration à l'autorité compétente de protection des données. Aujourd'hui, le transfert des données à destination ou en provenance de l'Union européenne a été renforcé et doit se faire dans le respect des règles du RGPD[417].

***182. Des règles spécifiques au transfert de données hors de l'Union européenne***. Le principe général défendu à l'article 44 du RGPD englobe le cas de la sous-traitance et les transferts ultérieurs afin de couvrir l'ensemble de la chaîne du transfert des données personnelles. Il est exigé, alors, que le niveau de protection des personnes physiques tel que garanti par le Règlement ne soit pas compromis, y compris en cas de transferts ultérieurs de données à caractère personnel au départ ou vers des pays tiers[418]. Ce principe se veut donc d'une application large afin d'étendre le niveau de protection à un maximum de situations.

***183.*** Les garanties posées par le RGPD ont pour but d'assurer le respect des exigences en matière de protection des données et des droits des personnes concernées avec la consécration de droits opposables, de voies de droit effectives telles que le droit d'engager un recours administratif ou juridictionnel, introduire une action en réparation. Dans le cadre d'un transfert de données à caractère personnel vers un pays tiers, le responsable du traitement ou le sous-traitant doit informer la personne concernée des garanties appropriées ainsi que les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition. La délivrance de ces informations est une obligation positive à la charge du responsable du traitement des données et du sous-traitant. Le RGPD n'interdit, donc, pas le transfert des données hors de l'Union européenne, mais exige que ce transfert s'inscrive dans le cadre défini par le RGPD. À ce titre, le RGPD prévoit des mécanismes pour autoriser le transfert des données hors de l'Union européenne.

***184.*** Il en résulte qu'il existe plusieurs conditions alternatives pour pouvoir transférer les données hors de l'Union européenne et satisfaire, ainsi, à l'exigence « d'un niveau de protection adéquat » lesquelles sont abordées dans la partie suivante.

---

[416] V. art. 68 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004 : « Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat n'appartenant pas à la Communauté européenne que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet. Le caractère suffisant du niveau de protection assuré par un Etat s'apprécie en fonction notamment des dispositions en vigueur dans cet Etat, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées ».

[417] En particulier les règles définies au chapitre V du RGPD.

[418] V. art. 44 du RGPD.

**2) L'extraterritorialité en matière de transfert de données à l'international**

***185. Les conditions du transfert des données hors de l'Union européenne.*** Le RGPD prévoit les conditions pour réaliser un transfert de données à caractère personnel hors de l'Union européenne, lesquelles sont étudiées ci-dessous.

***186. Un transfert autorisé sur décision d'adéquation par la Commission***. Un transfert pourra avoir lieu hors de l'Union européenne sur décision d'adéquation de la Commission. C'est l'article 45 du RGPD[419] qui énonce la procédure à suivre et les conditions à remplir. Il est prévu qu'un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question, assure un niveau de protection adéquat. La question se pose, donc, de savoir comment la Commission évalue le critère « du niveau de protection adéquat ». Il est précisé au même article[420] qu'elle tient compte, de plusieurs critères tels que l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation, les règles professionnelles et les mesures de sécurité, la jurisprudence, les droits effectifs et les recours des personnes concernées, l'existence de(s)autorités de contrôle indépendantes[421], les engagements internationaux. La Commission utilise lesdits critères détaillés, ci-dessus, pour évaluer si le pays concerné dispose d'un niveau de protection adéquat et rend ensuite une décision d'adéquation autorisant le transfert des données hors de l'Union européenne (pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale). Si la Commission évalue que le pays concerné dispose d'un niveau de protection adéquat, une décision d'adéquation est rendue pour permettre le transfert de données à caractère personnel.

***187.*** Concernant la nature juridique de cette décision, il s'agit d'un acte d'exécution dans lequel est précisé son champ d'application territorial et sectoriel et, le cas échéant, nomme la ou des autorités de contrôle. À la suite, de la décision d'adéquation, la Commission publie au Journal officiel de l'Union européenne et sur son site internet une liste des pays tiers, des territoires et des secteurs déterminés dans un pays tiers et des organisations internationales pour lesquels elle a constaté par voie de décision qu'un niveau de protection adéquat est ou n'est plus assuré. Si la Commission européenne ne se prononce pas sur une décision d'adéquation, alors il faut se

[419] V. art. 45 du RGPD ; pour déterminer si le pays concerné dispose d'un niveau de protection adéquat, la Commission utilise les critères tels que l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, l'existence d'autorités de contrôle indépendantes, les engagements internationaux pris (…). La Commission pourra émettre une décision d'adéquation dès lors qu'elle aura constaté dans le cadre d'une évaluation du caractère adéquat du niveau de protection de l'entité concerné (un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou une organisation internationale).

[420] Ibid.

[421] La CNIL en Irlande, « Information Commissioner's Office » au Irlande et « lIrlande en Espagne.

référer au deuxième mécanisme offert par le RGPD permettant de transférer les données hors de l'Union européenne.

***188.*** ***Un transfert autorisé moyennant des garanties appropriées***. En application de l'article 46 du RGPD[422], pour pouvoir transférer des données hors de l'Union européenne, en l'absence d'une décision d'adéquation de la Commission européenne, le responsable du traitement ou le sous-traitant devra adopter des solutions qui garantissent aux personnes concernées des droits opposables et effectifs en ce qui concerne le traitement de leurs données dans l'Union une fois que ces données ont été transférées, de façon à ce que lesdites personnes continuent de bénéficier des droits fondamentaux et des garanties[423]. En l'absence d'une décision d'adéquation, il demeure toujours possible d'effectuer un transfert, mais dans ce cas, « le responsable du traitement ou le sous-traitant doit prendre des mesures pour compenser l'insuffisance de la protection des données dans le pays tiers par "des garanties appropriées" en faveur de la personne concernée »[424]. Ces garanties appropriées peuvent prendre plusieurs formes telles qu'énoncées à l'article 46 du RGPD[425]. Il est possible de scinder ces garanties en deux catégories.

***189.*** Tout d'abord, il existe les garanties appropriées qui ne nécessitent pas d'autorisation particulière d'une autorité de contrôle ; il peut s'agir, soit d'un instrument juridiquement contraignant exécutoire entre les autorités ou organismes publics, soit des règles d'entreprise contraignantes, soit des clauses types de protection des données adoptées par une autorité de contrôle et approuvées par la Commission, soit un code de conduite approuvé, soit un mécanisme de certification approuvé.

***190.*** Ensuite, il existe des garanties appropriées qui requièrent une autorisation de contrôle de l'autorité compétente; il peut s'agir, soit de clauses contractuelles entre le responsable du traitement ou le sous-traitant et le responsable du traitement, le sous-traitant et le destinataire des données à caractère personnel dans le pays tiers ou l'organisation internationale, soit de dispositions à intégrer dans des arrangements administratifs entre les autorités publiques ou les organismes qui prévoient des droits opposables et effectifs pour les personnes concernées. En l'espèce, il est précisé que ces garanties devraient en particulier porter sur le respect des principes généraux concernant le traitement des données à caractère personnel et des principes de protection des données dès la conception et de protection des données par défaut.

---

[422] V. art. 46 du RGPD.

[423] V. considérant 114 du RGPD.

[424] V. considérant 108 du RGPD.

[425] V. art. 46 du RGPD.

***191.*** En conséquence, il est possible, en application de l'article 46 du RGPD, de transférer les données à caractère personnel vers un pays tiers ou une organisation syndicale lorsque le responsable du traitement ou le sous-traitant a prévu « des garanties appropriées » et à la condition que les personnes concernées disposent de droits opposables et des voies de droits effectifs.

***192.*** Concernant le transfert de données à caractère personnel en présence de règles d'entreprise contraignantes, le RGPD détaille la procédure à suivre.

***193. Un transfert autorisé par l'établissement de règles d'entreprise contraignantes***. En l'absence d'une décision d'adéquation, la Commission peut autoriser le transfert lorsque sont mises en place des règles d'entreprise contraignantes[426]. L'article 4, 20, du RGPD définit les règles d'entreprise contraignantes, ou BCR[427] comme «les règles internes relatives à la protection des données à caractère personnel qu'appliquent un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre pour des transferts ou pour un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant établi dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe»[428].

***194.*** Ces règles consistent à garantir au sein d'un groupe d'entreprise le respect du cadre européen de protection des données lors des transferts et traitements des données provenant d'une entité du groupe située sur le territoire de l'Union européenne. En application de l'article 47 du RGPD, il faut que « ces règles d'entreprise (ou BCR/Binding Corporate Rules)[429] soient juridiquement contraignantes, et soient mises en application par toutes les entités concernées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe, y compris leurs employés ; qu'elles confèrent expressément aux personnes concernées des droits opposables en ce qui concerne le traitement de leurs données à caractère personnel ; qu'elles précisent la structure et les coordonnées du groupe d'entreprises ou des groupes d'entreprises, les transferts ou l'ensemble des transferts de données, leur nature juridiquement contraignante, tant en interne qu'en externe, l'application des principes généraux relatifs à la protection des données, les droits des personnes concernées à l'égard du traitement et les moyens d'exercer ces droits, l'acceptation par le responsable du traitement ou le sous-traitant de l'engagement de sa responsabilité pour toute violation des règles d'entreprise

[426] V. art. 47 du RGPD relatif aux règles d'entreprise contraignantes.

[427] Binding Corporate Rules.

[428] V. art. 4, 20 du RGPD.

[429] V. Naftalski F., Les BCR « sous-traitants » consacrés paR le Groupe de l'article 29 : un grand pas en avant pour sécuriser les transferts internationaux de données dans le cadre du cloud computing, RLDI 2012/85, nº 2870.

contraignantes, la manière dont les informations sont fournies aux personnes concernées, les procédures de réclamation, les mécanismes pour garantir le contrôle du respect des règles d'entreprise contraignantes, les mécanismes pour communiquer et consigner les modifications apportées aux règles et pour communiquer ces modifications à l'autorité de contrôle, le mécanisme de coopération avec l'autorité de contrôle mis en place pour assurer le respect des règles par toutes les entités du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, notamment en mettant à la disposition de l'autorité de contrôle les résultats des contrôles des mesures pour garantir le respect des règles d'entreprise contraignantes, la formation appropriée en matière de protection des données pour le personnel ayant un accès permanent ou régulier aux données à caractère personnel. Concernant la procédure, il est exigé conformément au mécanisme de contrôle de l'article 63 du RGPD que l'autorité de contrôle compétente approuve ces règles d'entreprise contraignantes et que cette approbation ne peut intervenir que sous certaines conditions, lesquelles sont illustrées à l'article 47 du RGPD.

***195.*** Il en résulte que sous certaines conditions[430], il sera possible d'effectuer un transfert de données international, au sein d'une même entité économique, dès lors que cette entité recourt à des règles d'entreprise contraignantes approuvées pour ses transferts internationaux de l'Union vers des entités du même groupe d'entreprises. L'exigence, dans cette situation, est l'adoption des règles d'entreprise contraignantes qui doivent inclure les principes essentiels de protection des données et les droits opposables pour assurer des garanties appropriées pour les transferts de données à caractère personnel. Ces règles d'entreprise contraignantes doivent, aussi, prévoir la possibilité de transférer des données dans certains cas, à savoir : la personne concernée a donné son consentement explicite, ou lorsque le transfert est occasionnel, ou nécessaire dans le cadre d'une action en justice, ou en présence de motifs importants d'intérêt public ou lorsque le transfert intervient au départ d'un registre établi par la loi et destiné à être consulté par le public ou par des personnes ayant un intérêt légitime. Toutes ces dérogations sont accordées soit pour des motifs d'intérêt public ou pour protéger un intérêt essentiel et pour des transferts qualifiés de non répétitifs.

***196.*** S'il existe des règles européennes en matière de transfert de données à caractère personnel de l'Union européenne vers des pays tiers, l'effectivité de celles-ci peuvent être remise en cause par la mise en œuvre d'une loi ou d'une décision de justice étrangère.

[430] V. considérant 111 du RGPD.

***197. La prééminence théorique des règles européennes sur les règles étrangères***. Concernant l'exécution des décisions des juridictions et des autorités publiques étrangères, l'article 48 du RGPD dispose que « toute décision d'une juridiction ou d'une autorité d'un État tiers exigeant la divulgation ou le transfert de données personnelles protégées par le RGPD ne peut être reconnue ou rendue exécutoire que si elle est fondée sur les stipulations d'un traité qui lie cet État tiers avec l'Union européenne ou l'un de ses États membres »[431]. À la lecture de cette disposition, il n'apparaît pas que le droit d'un État tiers puisse être un fondement licite pour autoriser le transfert,[432] mais permet de faire produire les effets d'une décision de justice étrangère ou d'une autorité d'un État tiers sous certaines conditions. Sur ce point, la doctrine a considéré que « l'effectivité d'une telle prééminence juridique conférée aux règles du RGPD par de telles dispositions demeure toutefois largement théorique »[433]. L'effectivité théorique des règles européennes réside, ici, par l'admission de faire produire des effets juridiques à une décision de justice étrangère ou d'une autorité d'un État tiers. Concernant cette effectivité théorique des règles européennes, la doctrine ajoute qu'« en dépit des sanctions prévues par le règlement en cas de violation de l'une des dispositions précitées, l'effectivité réelle du texte semble irréductiblement être fonction des rapports de force entre grandes puissances»[434]. Effectivement, cette affirmation doctrinale a pu être vérifiée dans la documentation contractuelle[435] de la société Amazon[436]. Précisément, dans cette documentation, il est précisé qu'Amazon ne limite pas « la possibilité de divulgation aux seuls cas où cela est requis par le droit de l'Union ou d'un État membre, conformément aux dispositions de l'article 28.3 précitées, mais l'étend à toute décision d'une autorité gouvernementale (« governmental body ») sans autre précision - laquelle peut donc relever d'un pays tiers extérieur à l'Union - exposant par là ses clients à une violation de l'article 28 précité, entendu dans son sens le plus strict »[437]. Il en résulte de cette disposition contractuelle, qu'Amazon se soumet, pour la divulgation des

[431] Article 48 du RGPD.

[432] Deroudille A' et Fatah F., L'extraterritorialité du RGPD dans le contexte du « Cloud Act », Rev. UE 2019. n°442.

[433] Ibid.

[434] Ibid.

[435] Précisément, l'annexe « Data processing adde119rese» dans son offre de sous-traitance: « AWS will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental bodysends AWS a demand for Customer Data, AWS will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, AWS may 'rovide Customer's basic contact information to the government body. If compelled to disclose Customer Data to a government body, then AWS will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless AWS is legally prohibited from doing so.If the Standard Contractual Clauses apply, nothing in this Section 3 varies or modifies the Standard Contractual Clauses » ; « Data Process'ng Addendum » d'AWS, art. 3 ; https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR DPA.pdf/.

[436] AWS : Amazon Web Services

[437] Deroudille A' et Fatah F., L'extraterritorialité du RGPD dans le contexte du « Cloud Act », Rev. UE 2019. n°442.

données, non seulement au droit de l'Union européenne ou d'un État membre, mais aussi à toute autorité étrangère d'un pays tiers extérieur à l'Union européenne.

***198.*** En outre, les pays tiers vers lesquels sont transférées les données peuvent adopter des lois, des règlements ou d'autres actes juridiques visant à réglementer les activités de traitement des données effectuées par des personnes relevant de la compétence des États membres et pourraient être contraires au droit international et au RGPD. La réglementation de ce pays tiers peut, ainsi, faire obstacle à la protection des données des personnes physiques garantie dans l'Union européenne par le présent règlement. Le transfert des données à caractère personnel hors des frontières de l'Union européenne peut présenter un risque concernant la protection des données et l'exercice des droits des personnes concernées. C'est pour éviter une telle situation, qu'il est exigé dans le RGPD que le transfert des données hors de l'Union européenne ne doit être autorisé que lorsque les conditions ainsi fixées par le présent règlement sont remplies. Mais en pratique, il apparaît que la prééminence des règles européennes sur les règles étrangères et en particulier étasuniennes est uniquement théorique.

***199. La capacité d'examen des autorités de contrôle en difficulté.*** Il existe une difficulté pratique concernant la capacité des autorités de contrôle de chaque pays pour examiner les réclamations et mener des enquêtes, et ce en raison de l'hétérogénéité des régimes juridiques. C'est en partie pour cette raison et pour pallier cette difficulté que le RGPD met en avant le renforcement d'une coopération internationale. Il est précisé que « les autorités de contrôle devraient coopérer entre elles et avec la Commission »[438] et organiser « une coopération entre les autorités de contrôle-chef de file et les autres autorités de contrôle concernées dénommé « mécanisme de guichet unique »[439]. Il est indiqué que cette coopération doit se manifester par la prise de mesures appropriées pour élaborer les mécanismes de coopération internationale, se prêter mutuellement assistance sur le plan international, associer les parties prenantes intéressées aux discussions et activités visant à développer la coopération internationale, favoriser l'échange et la documentation de la législation et des pratiques en matière de protection des données. En revanche, tel que souligné par Monsieur Deroudille et Monsieur Fatah, « l'économie numérique et les enjeux liés aux données étant par nature transnationaux, l'on ne peut faire l'économie d'une analyse de l'application extraterritoriale du RGPD et de la protection des données sujettes aux transferts internationaux. Ces transferts peuvent faire l'objet d'une double compétence des autorités européennes et américaines »[440].

[438] V. considérant 123 du RGPD.

[439] V. considérant 127 du RGPD.

[440] Deroudille A et Fatah F., L'extraterritorialité du RGPD dans le contexte du « Cloud Act », Rev. UE 2019. n°442.

***200. La mise en œuvre difficile du droit à l'oubli.*** Il a pu être révélé des limites territoriales à la mise en œuvre du droit de la personne concernée, en particulier, concernant le droit à l'oubli sur internet. Sur ce point, la CNIL a entrepris un combat pour que « le droit au déréférencement ait une portée élargie aux extensions de noms de domaine en dehors du seul territoire français s'est soldé par une demi-victoire devant la Cour de justice[441]. Si celle-ci a, en effet, considéré qu'un déréférencement à l'échelle de l'Union pouvait être imposé à Google, elle a, en revanche, estimé qu'il n'était pas possible, sur le fondement du droit européen, d'imposer ce mécanisme au-delà, conduisant concrètement à ce qu'une information, qui pourtant relève de ce droit à l'oubli, demeure disponible sur Internet à partir d'un nom de domaine ayant une extension non européenne »[442]. Si cette décision est salutaire, en revanche, elle laisse une possibilité, « de déroger par le haut »[443] ce qui peut affaiblir la démarche d'une harmonisation du régime de protection des données à caractère personnel. Concernant l'affaiblissement d'un régime européen de protection uniforme des données, certains auteurs ont considéré « que le concept même de « règlement » en ressort galvaudé[444]. Certes, la Cour de justice, en invalidant les instruments relatifs aux transferts internationaux des données[445], tente de sanctuariser la protection de ses citoyens, en s'assurant que les actes passés par les institutions européennes elles-mêmes ne vident pas la protection de toute substance, mais force est de reconnaître que le marché unique de la donnée personnelle fuit de toutes parts »[446]. Le constat, ici, pourrait en dire long quant au système juridique européen mis en place pour assurer la protection des données à caractère personnel. L'Union européenne serait dans l'incapacité à garantir une protection effective du droit à la protection des données à caractère personnel dès lors que les États-Unis ne se soumettent pas à la réglementation nationale et européenne.

---

[441] CJUE 24 sept. 2019, aff. C-507/17, *Google LLC / CNIL* (Arrêt rendu à la suite d'une question préjudicielle posée par le Conseil d'État du 15 mars 2017, *G.C., A.F., B.H., E.D. c/ CNIL).*

[442] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279.

[443] CE 27 mars 2020, n° 399922, Lebon : le CE avait refusé faute pour la loi française d'offrir, en l'état, le fondement adéquat.

[444] Ancel M.-E., D'une diversité à l'autre, À propos de la « marge de manœuvre » laissée par le Règlement général sur la protection des données aux États membres de l'Union européenne, Rev. crit. DIP 2019. 647. Jacob P, La compétence des États à l'égard des données numériques : du nuage au brouillard... en attendant l'éclaircie ? Rev. crit. DIP 2019. 665 ; Mantovani M., Le RGPD en tant qu'espace juridique multi-échelle : quelles implications pour le droit international privé ? Revue de droit international d'Assas n° 2, déc. 2019, p. 4.

[445] CJUE 6 oct. 2015, aff. C-362/14, *Schrems I*, AJDA 2015. 2257, chron. Broussy E., Cassagnabère H. et Gänser C.; CJUE 16 juill. 2020, aff. C-311-18, *Data protection Commissioner c/ Maximillian Schrems et Facebook Ireland*. V. not. Perray R., *Schrems II* : adéquation et caractère approprié des clauses contractuelles types, l'*accountability* met en balance , RLDI, n° 169, 2020. 35 ; Martial-Braz N., Nouvelle donne en matière de transfert de données personnelles hors Union européenne, JCP n° 41, 5 oct. 2020, p. 1116.

[446] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279.

***201.*** En conséquence, il est nécessaire en application de ces textes d'observer le niveau de protection des données à caractère personnel accordé aux personnes physiques.

***202.*** Après avoir étudié les règles européennes relatives au transfert des données au sein et hors de l'Union européenne, il est envisagé d'étudier les règles étrangères en matière de protection des données, en particulier les règles étasuniennes.

## B) Les règles américaines du transfert de données à caractère personnel

***203.*** À titre de comparaison avec le cadre réglementaire de l'Union européenne pour la protection des données à caractère personnel, les États-Unis ne disposent pas, au niveau fédéral, d'une réglementation générale pour la protection des données à caractère personnel (1) en revanche, il existe des réglementations sectorielles au niveau des états fédérés (2).

### 1) L'absence d'une réglementation générale relative à la protection des données à caractère personnel au niveau de l'État fédéral

***204.*** L'Union européenne dispose d'une réglementation générale pour la protection des données à caractère personnel alors que les États-Unis en sont dépourvus. Cette absence de protection peut susciter des interrogations et des inquiétudes dès lors qu'un transfert de données est opéré de l'Union européenne vers les États-Unis. Ces inquiétudes sont perceptibles en doctrine et à ce sujet, E. Netter met en lumière l'existence "d'un affrontement des modèles : un choc des souverainetés (…) puisqu'il semble aujourd'hui très difficile d'assurer à un export de données hors de l'Union européenne une sécurité juridique satisfaisante à long terme, quelles conséquences faut-il en tirer ? Ces flux doivent-ils tout simplement cesser ? Les grandes multinationales doivent-elles mettre en place deux circuits de traitement de données totalement hermétiques l'un à l'autre : un pour l'Europe, un pour le reste du monde ? (..) Entre les modèles européen et américain, la tension continue à monter"[447]. Également, la doctrine soulève des interrogations en la matière et rappelle que « force est de constater que, du fait du recours à la sous-traitance, la fuite des données en direction de ces personnes morales de droit américain est aujourd'hui généralisée. En effet, quelle entreprise ne fait pas appel aux services de Google Cloud, d'AWS (Amazon), Microsoft One note, ou bien encore Salesforce pour conserver et

[447] Netter E., Regards sur le nouveau droit des données personnelles, édition CEPRISCA, Collection Colloques, novembre 2019. V. également, Naftalski F. et Desgens-Pasanau G', Le cloud computing à l'épreuve des souverainetés nationales, RLDI 2013/90, nº 3006.

traiter ses fichiers clients ou bien toutes les autres données personnelles qu'elle détient ? »[448]. Dans le cadre d'une analyse comparative, il apparaît que les États-Unis sont dépourvus au niveau fédéral d'une réglementation générale protectrice des données à caractère personnel,[449] mais garantissent la vie privée et la protection des données à travers d'autres actes, tels que « the United States Privacy Act 2020 »[450], « the Privacy Shield »[451], « the Health Insurance Portability and Accountability Act of 1996 »[452].

***205.*** La particularité des États-Unis, pour appréhender la protection des données, consiste à adopter une approche par secteur[453]. Il a été adopté des lois *ad hoc*, telles que « the Video Privacy Protection Act of 1988 », « the Cable Television Protection » and « Competition Act of 1992 », and « the Fair Credit Reporting Act » [454]. Il est, ainsi, fait le choix aux États-Unis d'une

---

[448] Deroudille A. et Fatah F., L'extraterritorialité du RGPD dans le contexte du « Cloud Act », Rev. UE 2019. n°442.

[449] Concernant la tradition juridique aux USA s'agissant de la protection des données: « The reasoning behind the U.S. approach to privacy laws has as much to do with American laissez-faire economics as with its legal tradition. For example, while the U.S. has prized its right to free speech so dearly that the very first amendment to the U.S. Constitution protects it explicitly, the Constitution does not have an explicit right to privacy. The U.S. Supreme Court has found a right to privacy implied by the terms of other portions of the Constitution, and many states have explicit privacy rights in their state constitutions, but on a federal level there is no express constitutional guarantee to privacy. As a result, there is similarly no constitutional framework upon which to build a single data privacy act, making the ad hoc approach much more compatible in the American system" traduit en français par : Le raisonnement qui sous-tend l'approche américaine des lois sur la protection de la vie privée a autant à voir avec le laissez-faire économique américain qu'avec sa tradition juridique. Par exemple, si les États-Unis attachent tellement d'importance à leur droit à la liberté d'expression que le tout premier amendement de la Constitution américaine le protège explicitement, la Constitution ne prévoit pas de droit explicite à la vie privée. La Cour suprême des États-Unis a trouvé un droit à la vie privée implicite dans les termes d'autres parties de la Constitution, et de nombreux États ont des droits explicites à la vie privée dans leurs constitutions d'État, mais au niveau fédéral, il n'existe aucune garantie constitutionnelle expresse à la vie privée. Par conséquent, il n'existe pas non plus de cadre constitutionnel sur lequel construire une loi unique sur la protection des données, ce qui rend l'approche ad hoc beaucoup plus compatible avec le système américain : https://www.hg.org/data-protection.html.

[450] Apperçu de la loi "PRIVACY ACT" de 1974 (United States department of justice overview of the privacy act of 1974) edition 2020 (https://www.justice.gov/Overview_202'/download).

[451] Décision d'exécution (ue) 2016/1250 de la commission du 12 juillet 2016 conformément à la directive 95/46/ce du parlement européen et du conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE États-Unis, numéro C (2016) 4176 : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016D1250&qid=1620661087772&from=EN.

[452] Contenu de la loi « the Health Insurance Portability and Accountability Act of 1996 »: https://www.cdc.gov/phlp/publications/topic/hipaa.html.

[453] Concernant l'approche sectorielle des USA: "The United States follows 'hat is referred to as a 'sectoral' approach to data protection legislation. Under this approach, the laws of data protection and privacy rely on a combination of legislation, regulation, and self-regulation rather than governmental interference alone. Since the Clinton administration, the U.S. has followed a policy geared toward allowing the private sector to lead the way in data protection. This means that companies should implement their own policies, develop their own technology, and individuals should self-regulate to prevent the dissemination of their private data. Pursuant to this policy, the US has not yet developed a single, federal data protection law", traduit en français par : Les États-Unis suivent ce que l'on appelle une approche "sectorielle" de la législation sur la protection des données. Selon cette approche, les lois sur la protection des données et de la vie privée reposent sur une combinaison de législation, de réglementation et d'autoréglementation plutôt que sur la seule intervention gouvernementale. Depuis l'administration Clinton, les États-Unis ont suivi une politique visant à permettre au secteur privé de montrer la voie en matière de protection des données. Cela signifie que les entreprises doivent mettre en œuvre leurs propres politiques, développer leurs propres technologies et que les individus doivent s'autoréguler pour empêcher la diffusion de leurs données privées. Conformément à cette politique, les États-Unis n'ont pas encore élaboré de loi fédérale unique sur la protection des données : https://www.hg.org/data-protection.html.

[454] Concernant l'application des lois ad hoc "U.S. Ad Hoc Privacy Laws: Under the U.S. Sectoral approach, however, privacy legislation tends to be sparse and only adopted on an ad hoc basis, with legislation arising when circumstances require. These laws usually only apply to situations in which individuals would not be able to control the use of their data through self-regulations. Examples include the Video Privacy Protection Act of 1988, the Cable Television Protection and Competition Act of 1992, and the Fair Credit Reporting Act"; traduit en français par "Les lois ad hoc sur la protection de la vie privée aux États-Unis : Dans le cadre de l'approche sectorielle américaine, cependant, la législation sur la protection de la vie privée tend à être peu abondante et à n'être adoptée que sur une base ad hoc, la législation apparaissant lorsque les circonstances l'exigent. Ces lois ne s'appliquent généralement qu'aux situations dans lesquelles les individus ne seraient pas en mesure de contrôler l'utilisation de leurs données par le biais

non-immixtion de l'État fédéral, en matière de protection des données à caractère personnel, dans la vie des entreprises. Les entreprises disposent, alors, de la liberté d'établir elles-mêmes la politique de protection des données personnelles qu'elles s'engagent à respecter et à mettre en œuvre. L'explication de la non-immixtion de l'État fédéral dans la vie des entreprises tient à la tradition juridique des États-Unis. En effet, si la liberté d'expression est le premier amendement de la constitution américaine[455], celle-ci n'a pas consacré le droit à la vie privée. En revanche, la Cour Suprême des États-Unis a pu faire ressortir un droit à la vie privée en se basant sur d'autres dispositions de la Constitution

**2) L'existence d'une réglementation sectorielle pour la protection des données à caractère personnel au niveau des États fédérés**

***206.*** Si au niveau fédéral des États-Unis, il a été observé l'absence d'une réglementation générale protectrice des données à caractère personnel, il a été constaté, en revanche, qu'au niveau des États fédérés, certains États ont consacré dans leur constitution un droit à la vie privée, mais ces lois ne sont applicables que dans l'état concerné[456]. À titre d'exemple, la Californie a adopté le 28 juin 2018, le *California Consumer Privacy Act (CCPA)* ; il s'agit d'une loi pour la protection du consommateur de Californie et intègre la protection des données à caractère personnel du consommateur[457]. Les conditions de mise en œuvre de cette loi sont strictes puisqu'elle

---

d'autorégulations. Parmi les exemples, citons le Video Privacy Protection Act de 1988, le Cable Television Protection and Competition Act de 1992 et le Fair Credit Reporting Act" : https://www.hg.org/data-protection.html Texte de cette loi "the Fair Credit Reporting Act" : https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf.

[455] First Amendment « Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances »; traduit en français par "Le Congrès ne fera aucune loi concernant l'établissement d'une religion ou interdisant son libre exercice, ou restreignant la liberté de parole ou de la presse, ou le droit du peuple de s'assembler pacifiquement et d'adresser des pétitions au gouvernement pour un redressement des griefs" : https://constitution.congress.gov/browse/amendment-1/.

[456] https://www.hg.org/data-protection.html : "Data Protection Law deals with the security of the electronic transmission of personal data. Yet, the United States does not have any centralized, formal legislation at the federal level regarding this issue, but does insure the privacy and protection of data through the United States Privacy Act, the Safe Harbor Act and the Health Insurance Portability and Accountability Act"; traduit en français par "La loi sur la protection des données traite de la sécurité de la transmission électronique des données personnelles. À ce jour, les États-Unis n'ont pas encore de législation centralisée et officielle au niveau fédéral concernant cette question, mais ils assurent la confidentialité et la protection des données par le biais de la loi américaine sur la protection de la vie privée, de la loi sur la sphère de sécurité et de la loi sur la portabilité et la responsabilité en matière d'assurance maladie ».

[457] Concernant le contenu de cette loi « The California Consumer Privacy Act of 2018 (CCPA) gives consumers more control over the personal information that businesses collect about them. This landmark law secures new privacy rights for California consumers, including: The right to know about the personal information a business collects about them and how it is used and shared; The right to delete personal information collected from them (with some exceptions);The right to opt-out of the sale of theand thesonal information; andThe right to non-discrimination for exercising their CCPA rights. Businesses are required to give consumers certain notices explaining their privacy practices. The CCPA applies to many businesses, including data brokers" ; nous traduisons par « La loi californienne de 2018 sur la protection de la vie privée des consommateurs (CCPA) donne aux consommateurs davantage de contrôle sur les informations personnelles que les entreprises collectent à leur sujet. Cette loi historique garantit de nouveaux droits à la vie privée pour les consommateurs californiens, notamment : Le droit de connaître les informations personnelles qu'une entreprise collecte à leur sujet et la manière dont elles sont utilisées et partagées ; Le droit de supprimer les informations personnelles collectées à leur sujet (avec quelques exceptions) ; Le droit de refuser la vente de leurs informations personnelles ; et Le droit à la non-

s'applique uniquement aux « entreprises implantées en Californie qui atteignent des revenus de 25 millions ou qui collectent des données d'au moins 50 000 consommateurs ou dont la moitié de leurs revenus provient de la vente des données personnelles »[458]. Autrement dit, il ne s'agit pas d'une loi d'application générale à la protection des données à caractère personnel et sa portée est limitée par rapport à la réglementation européenne. À ce sujet, il a été considéré par des auteurs que "si cette loi accorde plus de droits que la plupart des lois sectorielles applicables aux États-Unis, ces droits restent plus limités qu'en Europe. Le droit des individus d'interdire la revente de leurs données lors de la conclusion d'un contrat (*opt out*) fait figure de progrès, mais est encore bien éloigné des standards du droit de l'Union"[459]. D'autres États prennent, également, le même chemin que la Californie, tels que Washington[460]. Ces lois sectorielles accordent des prérogatives au consommateur pour la protection des données à caractère personnel, mais n'édictent pas de règles générales relatives à la protection des données à caractère personnel dans le cadre d'un transfert des données.

***207.*** Après avoir constaté l'absence aux États-Unis d'une réglementation générale pour la protection des données à caractère personnel, la question se pose de savoir, tout d'abord, si un transfert de données à caractère personnel de l'Union européenne vers les États-Unis est autorisé et si oui quelles sont les conditions, puis, est-ce que ce transfert ne compromet pas les garanties du RGPD et donc l'effectivité des règles européennes en matière de protection des données.

## Section 2 : Les critiques de l'effectivité des règles européennes dans le cadre d'un transfert des données à caractère personnel

***208.*** Il est envisagé d'étudier l'effectivité des règles européennes en matière de transfert des données à caractère personnel hors de l'Union européenne, et ce au regard de l'impératif de protection des données dans les contrats de cloud computing. Il est fait le choix d'analyser l'effectivité des règles européennes de protection des données à caractère personnel par rapport à la réglementation étasunienne puisque ce sont les entreprises américaines qui dominent le marché des prestations de services de cloud computing.

---

discrimination pour l'exercice de leurs droits CCPA. Les entreprises sont tenues de fournir aux consommateurs certains avis expliquant leurs pratiques en matière de confidentialité. L'ACCP s'applique à de nombreuses entreprises, dont les courtiers en données ». https://oag.ca.gov/privacy/ccpa.

[458] Recueil Dalloz, *Schrems II* et invalidation du *Privacy Shield*, *un goût de « déjà vu »*…, Castets-Renard C. – D. 2020. 2432

[459] Ibid.

[460] Ibid.

***209.*** **Plan.** S'agissant de l'établissement des critiques relatives à l'effectivité des règles européennes de protection des données à caractère personnel, il apparaît que celles-ci sont fondées d'une part sur l'hégémonie réglementaire étasunienne (A) et d'autre part sur le montage contractuel opéré par les prestataires de services cloud (B).

## A) Une critique fondée sur l'hégémonie réglementaire des États-Unis

***210.*** Après avoir constaté l'absence aux États-Unis d'une réglementation générale pour la protection des données à caractère personnel, cette partie traite la question de savoir si un transfert de données à caractère personnel de l'Union européenne vers les États-Unis est autorisé et si oui quelles sont les conditions. Il apparaît, tout d'abord, que les lois sécuritaires américaines ont une incidence directe quant à l'effectivité des règles européennes sur la protection des données en raison de la primauté des premières sur les secondes (1) puis, que cette incidence n'a pas pour conséquence, pour autant, d'empêcher le transfert des données de l'Union européenne vers les États-Unis (2).

### 1) La primauté des règles étasuniennes sur les règles européennes

***211.*** Il a été observé précédemment que les États-Unis ne disposent pas d'une réglementation générale pour la protection des données à caractère personnel contrairement à l'Union européenne avec le RGPD. La préoccupation des utilisateurs de services de cloud computing, en l'espèce les personnes physiques résidant sur le territoire européen, est de voir appliquer la réglementation étasunienne à leur contrat de cloud computing. Il est, ainsi, procédé à l'étude des sources légales aux États-Unis qui traitent de la question du transfert des données en particulier lorsque les données font l'objet d'un contrat de cloud computing par des utilisateurs (personnes physiques) résidant sur le territoire de l'Union européenne.

***212.*** **Plan.** En particulier, il est envisagé d'étudier l'affirmation (a) et la généralisation (b) du droit d'accès et de collecte des données à caractère personnel par les États-Unis.

#### a) L'affirmation du droit d'accès et de collecte des données des États-Unis

***213.*** Au niveau de l'État fédéral des États-Unis, la source légale utilisée pour exiger la communication des données de toute personne physique indépendamment de son lieu de résidence, est la loi *Foreign Intelligence Surveillance Act* du 25 octobre 1978, laquelle a pour acronyme FISA et a été amendée par le FISA Amendements Act 2008. Cette loi est toujours

d'application et accorde le droit aux États-Unis de demander aux opérateurs tels que Facebook, Google, de transmettre les métadonnées de leurs clients utilisant leurs services. Par cette loi les opérateurs américains ont l'obligation de transmettre sur demande aux autorités américaines les données qu'ils ont pu collecter sur leurs clients et ce peu importe si ces données concernent des personnes physiques résidant sur le territoire de l'Union européenne ou que ces données sont collectées depuis le territoire de l'Union européenne.

***214.*** Sur le fondement de cette loi FISA, les prestataires américains de services cloud sont soumis au respect de cette réglementation les obligeant à communiquer aux autorités américaines les données de clients qui sont hébergées dans leurs serveurs. Cette loi du Congrès américain édicte, également, « les procédures des surveillances physiques et électroniques, ainsi que la collecte d'information sur des puissances étrangères soient directement, soit par l'échange d'informations avec d'autres puissances étrangères »[461]. Le champ d'application des lois sécuritaires américaines est volontairement large pour couvrir le plus possible de situations. En renforcement de la loi FISA, il a été adopté le 26 octobre 2001 aux USA une autre loi antiterroriste appelée le USA PATRIOT Act[462]. En application de cette loi, le gouvernement américain dispose du droit de mettre la main sur les données stockées sur les serveurs d'entreprises américaines ou basées aux USA, et ce quel que soit le lieu où se trouvent effectivement ces données[463]. Le USA PATRIOT Act est le prolongement de la politique sécuritaire des États-Unis initiée par la loi FISA. En matière de contrat de cloud computing, dès lors que le prestataire de services cloud est une société américaine, le gouvernement américain a le droit d'exiger le transfert des données des utilisateurs, même si ces données concernent des résidents de l'Union européenne. Ce droit s'applique également à l'égard des prestataires de services cloud même s'ils ne sont pas des sociétés américaines dès lors que les données sont stockées dans des serveurs situés sur le territoire américain. En conséquence, les indicateurs à prendre en compte pour anticiper la mise en œuvre des prérogatives du gouvernement américain issues desdites lois sécuritaires sont, d'une part, la nationalité du prestataire de services cloud et d'autre part, le lieu

---

[461] The Foreign Intelligence Surveillance Act of 1978 prescribes procedures for requesting judicial authorization for electronic surveillance and physical search of persons engaged in espionage or international terrorism against the United Stat es on behalf of a foreign power; traduit en français par " La loi Foreign Intelligence Surveillance Act de 1978 prescrit les procédures de demande d'autorisation judiciaire pour la surveillance électronique et la fouille physique de personnes se livrant à l'espionnage ou au terrorisme international contre les États-Unis pour le compte d'une puissance étrangère » : https://fas.org/irp/agency/doj/fisa/.

[462] US PATRIOT Act (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act)*, Public Law 107–56—OCT. 26, 2001: nous traduisons par « loi pour unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme », loi publique 107-56 u 26 octobre 2001.

[463] Texte intégral de la loi « USA PATIOT ACT » : https://www.govinfo.gov/content/pkg/BILLS-107hr3162 nr/pdf/BILLS-107hr3162enr.pdf : le « Patriot act » lequel dispose que les agences de renseignement peuvent accéder à toute donnée personnelle hébergée par un prestataire américain en cas de suspicion de terrorisme ou d'espionnage. Ainsi, le Patriot Act rend difficilement applicable les principes de protection des données personnelles et rendent même inefficaces les clauses contractuelles de protection puisque les autorités américaines peuvent accéder et collecter ces données pour des raisons de sécurité nationale et de lutte contre le terrorisme. Le « Patriot Act » a permis au gouvernement de mettre la main sur des données stockées dans les serveurs d'entreprises américaines et ce quel que soit le lieu où se trouvent effectivement ces serveurs.

de la localisation des serveurs. Dès lors que le prestataire est une société américaine ou que les données collectées par des prestataires de services cloud non américains sont hébergées dans des serveurs situés aux États-Unis, le gouvernement américain dispose de prérogatives issues de ces lois sécuritaires.

***215.*** L'établissement de ces lois sécuritaires s'est poursuivi et se renforce au fil du temps et nous assistons même à un élargissement de son champ d'application.

b) La généralisation du droit d'accès et de collecte des données des États-Unis

***216.*** Dans la continuité du renforcement des précédentes lois sécuritaires[464], la loi fédérale américaine Cloud Act (*Clarifying Lawful Overseas Use of Data Act)*[465] permet « aux forces de l'ordre ou aux agences de renseignement américaines d'obtenir des opérateurs de télécommunication et des fournisseurs de services de Cloud computing des informations stockées sur leurs serveurs ; que ces données soient situées aux États-Unis ou à l'étranger »[466].

***217.*** À la différence du FISA, le champ d'application du « Cloud Act » ne se limite pas simplement aux personnes morales de droit américain, ou *« US persons »,* mais il s'étend aussi à des « non-US persons » c'est-à-dire à des personnes non américaines[467]. Ce nouveau texte « Cloud Act » est davantage sécuritaire que ne l'était le FISA en raison de l'élargissement de son champ d'application (« US Person et non US persons »). Cette loi permet encore, « à l'instar du RGPD, d'atteindre, via un critère de ciblage, les entreprises qualifiées de "providers of electronic communications services or remote computing services" dont le marché américain constitue la cible, c'est-à-dire, éventuellement certaines entreprises européennes, situées sur le territoire de l'Union — soit qu'elles soient des filiales européennes d'entreprise américaine, soit, au contraire, qu'elles ciblent un public américain, par exemple, via leurs filiales implantées

[464] La loi FISA (The Foreign Intelligence Surveillance Act) du 25 octobre 1978 et la loi USA PATRIOT Act du 26 octobre 2001.

[465] Cloud act (Clarifying Lawful Overseas Use of Data Act), nous traduisons par « loi clarifiant l'usage légal des données hébergées à l'étranger » promulguée le 23 mars 2018 laquelle est venue modifier « le chapitre 121 du Titre 18 du United States Code, dénommé Stored Communications Act.

[466] Gavetti J.-H., Le Cloud Act, la nouvelle loi sécuritaire des États-Unis, a de quoi inquiéter les autorités, les entreprises et les citoyens de l'Union européenne. En quoi consiste ce texte et pourquoi est-il à craindre ? cloud, juridique, les experts du numérique, publié le 1er février 2019 : https://www.usine-digitale.fr/article/le-cloud-act-un-texte-securitaire-americain-qui-inquiete.N800995. V. également, Rozenfeld S., Le Cloud Act : pour un accès extraterritorial aux données », Revue Expertises des systèmes d'information, 1er avril 2018, numéro 434, page(s) 123-124.

[467] Promoting Public Safety, Privacy, and the Rule of Law Around the World, The Purpose and Impact of the Cloud Act White Paper April 2019 ; traduit en français par « Promouvoir la sécurité publique, la vie privée et l'état de droit dans le monde, L'objectif et l'impact de Cloud Act, Livre blanc avril 2019 » : https://www.justice.gov/opa/press-release/file/1153446/download. Egalement, Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purp ose of Countering Serious Crime; traduit en français par « Accord entre le gouvernement des États-Unis d'Amérique et le gouvernement du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord sur l'accès aux données électroniques aux fins de la lutte contre la grande criminalité »: https://www.justice.gov/dag/cloud-act-agreement.

aux États-Unis »[468]. En l'espèce, les entreprises qualifiées de « providers of electronic communications services or remote computing services » peuvent être traduites par les fournisseurs de services de communications électroniques ou de services informatiques à distance. Avec ce texte, il est visé non seulement les sociétés américaines, mais aussi les sociétés européennes filiales de sociétés américaines et les sociétés européennes implantées aux États-Unis.

***218.*** L'objectif de ce texte est de généraliser et d'étendre plus largement le champ d'application des lois sécuritaires et de contribuer, ainsi, à renforcer l'hégémonie réglementaire étasunienne. Dans ce sens, le Cloud Act maintient les inquiétudes existantes et suscite des interrogations quant à la protection des données à caractère personnel de citoyens européens utilisant les services de cloud computing d'une entreprise américaine ou d'une société européenne dont les serveurs sont localisés aux États-Unis. À ce titre, la doctrine s'interroge sur la superposition du RGPD et du Cloud Act en matière « d'extraterritorialité de la norme juridique et par la même occasion d'efficacité de celle-ci sur un plus grand nombre de personnes »[469]. Il est mis en avant l'idée que « bien que les articles 28 et 48 du RGPD instituent, en quelque sorte, une prééminence théorique du droit européen de la protection des données sur les demandes de divulgation des juridictions et des administrations publiques des États tiers, l'effectivité réelle d'une telle disposition demeure problématique, notamment dans le contexte de l'adoption du « Cloud Act »[470]. Il est mis en lumière que si les États-Unis ont signé avec l'Union européenne un traité de coopération judiciaire, ce texte ne semble pas autoriser expressément les « perquisitions dans les conditions prévues par le « Cloud Act »[471]. Et à ce sujet, « la doctrine n'a pas manqué d'alerter sur le risque de violation du RGPD par une entreprise qui se conformerait à un mandat américain, ou, à l'inverse, d'une violation de ce même mandat en cas de refus de communication motivé par une volonté de conformité au texte européen »[472].

***219.*** En revanche, la réglementation européenne (et en particulier le RGPD) n'interdit pas aux États membres de conclure des accords internationaux pour autoriser le transfert de données de l'Union européenne vers un pays tiers[473]. Le RGPD habilite, également, la Commission pour émettre une décision d'adéquation au profit notamment d'un pays tiers[474] dès lors que ce pays

---

[468] Deroudille A., Les enjeux transatlantiques du RGPD à l'heure du Cloud act, publié le 2 septembre 2019 : https://deroudilleavocat.com/blog/2019/3/27/enjeu'transatlantiquesrgpd.

[469] Deroudille A. et Fatah F., L'extraterritorialité du RGPD dans le contexte du « Cloud Act », Rev. UE 2019. n°442.

[470] Ibid.

[471] Ibid.

[472] Ibid.

[473] V. considérant 102 du RGPD.

[474] V. art. 45 du RGPD.

dispose en particulier d'un niveau de protection adéquat au regard de certains critères tels que l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, l'existence d'autorités de contrôle indépendantes, les engagements internationaux pris. C'est dans le contexte d'établissement de lois sécuritaires par les Etats-Unis[475], qu'il a été négocié, entre le Département du Commerce américain et la Commission européenne, les principes de protection des données à caractère personnel fondés initialement sur ceux de la Directive 95/46 du 24 octobre 1995. Historiquement, avant l'adoption du règlement européen du 27 avril 2016, la réglementation nationale et européenne[476] interdisait le transfert des données hors de l'Union européenne sauf si le pays figurait sur la liste dérogatoire dressée par la Commission européenne. Pour figurer sur cette liste, le pays devait apporter la preuve que des garanties égales ou supérieures à celles des pays de l'Union européenne ont été prises pour la protection des données à caractère personnel. Parmi les pays figurants sur cette liste, les États-Unis n'en faisaient pas partie et devaient donc conclure des accords avec l'Union européenne pour autoriser le transfert de données personnelles.

***220.*** Entre l'Union européenne et les États-Unis, plusieurs accords ont vu le jour lesquels ont été remis en cause devant la Cour de justice de l'Union européenne, en raison de l'insuffisance du niveau de protection réservée aux données[477]. Nous aborderons dans cette partie la teneur de ces différents accords et leurs impacts quant à la protection des données personnelles dans les contrats de cloud de cloud computing.

**2) Un transfert autorisé des données de l'Union européenne vers les États-Unis**

***221.*** Face à l'adoption de ces législations sécuritaires américaines, et en particulier dans les années 1990 avec l'utilisation massive d'internet, la question s'est posée du niveau de la protection attachée aux données de citoyens européens lors d'un transfert vers les États-Unis. Très vite, des mécanismes ont été mis en place entre l'Union européenne et les États-Unis afin d'autoriser le transfert des données de l'Union européenne vers les États-Unis.

---

[475] La loi « Foreign Intelligence Surveillance Act (FISA) » du 25 octobre 1978, toujours d'application, laquelle a été amendée par le FISA Amendements Act 2008, accorde le droit aux États-Unis de demander aux opérateurs tels que Facebook, Google de transmettre les métadonnées des européens collectées depuis le territoire de l'Union européenne. https://fas.org/irp/agency/doj/fisa/. V. également, Le USA PATRIOT ACT « Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act – pouvant être'traduit en français par « Loi pour unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme ». Il s'agit d'une loi antiterroriste qui a été adoptée le 26 octobre 2001.

[476] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à carac ère personnel et à la libre circulation de ces données : JO 1995, L 281, p. 31.

[477] V. affaire Schrems 1, CJUE Data Protection Commissioner contre Maximillian Schrems et Facebook Ireland, 6 juillet 2020, affaire C-311/18, V. affaire Schrems 2 : CJUE, gr. ch., 6 oct. 2015, aff. C-362/ 4, Maximillian Schrems c/ Data Protection Commissioner : Décision de la CJUE invalidant le Sfe Harbor. V. également, CJUE Privacy International contre Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service, 6 octobre 2020, affaire C-623-17.

***222.*** **Plan.** Il est envisagé d'étudier l'insuffisance du niveau de protection des données par l'accord du Safe Harbor (a) du « EU-US. Privacy Shield » (b).

a) L'insuffisance du niveau de protection des données par l'accord du Safe Harbor

***223.*** L'Union européenne et les États-Unis ont signé un premier accord dénommé « SAFE HARBOR »[478] ou autrement nommé *« le Bouclier de confidentialité »* dont l'objet était d'encadrer l'utilisation des données des Européens et le transfert des données entre l'Union européenne et les États-Unis. Spécifiquement, cet accord avait pour objet d'édicter un régime juridique relatif au transfert de données privées transatlantique sur le fondement d'un mécanisme d'autocertification. Cet accord permettait, donc, aux entreprises établies aux États-Unis d'adhérer volontairement afin de pouvoir recevoir des données à caractère personnel en provenance de l'Union européenne[479]. Il s'agissait, ainsi, d'un mécanisme d'autorégulation auquel les entreprises pouvaient adhérer. Ce mécanisme permettait le transfert et le stockage des données entre l'Union européenne et les États-Unis. Les principes négociés figurant dans cet accord avaient, ainsi, pour objet d'établir un niveau de protection adéquat. La Commission européenne, dans sa Décision 200/520 du 26 juillet 2000 a considéré que le Safe Harbor offrait un niveau de protection adéquat des données[480] et a, donc, autorisé le transfert de données de l'Union européenne vers les États-Unis.

***224.*** À la suite de cette reconnaissance par la Commission et des révélations par Edward Snowden du programme de surveillance PRISM[481], l'accord du Safe Harbor a été remis en cause depuis la plainte déposée Maximillian Schrems devant la Cour de justice de l'Union européenne (CJUE). Il a été révélé qu'en application du USA Patriot Act, la NSA pouvait effectuer une collecte indifférenciée des données à caractère personnel sur internet « sans que celle-ci ne soit

[478] Décision de la Commission européenne numéro 200/520 du 26 juillet 2000 dans laquelle elle a considéré que le « Safe Harbor » ou autrement nommé « *le Bouclier de confidentialité* » offrait un niveau de protection adéquat des données transférées en provenance de l'Union européenne vers des en reprises établies aux États-Unis.

[479] Accord *SAFE HARBOR* : « Négociés entre les autorités américaines et la Commission européenne en 2001, le *Safe Harbor* est un ensemble de principes de protection des données personnelles. Ces règles publiées par le Département du Commerce américain, sont essentiellement basés sur ceux de la Directive 95/46 du 24 octobre 1995. Les entreprises établies aux Etats-Unis adhèrent volontairement afin de pouvoir recevoir des données à caractère personnel en provenance de l'Union. Le Safe Harbor permet donc à une entreprise américaine de certifier que le pays respecte la législation européenne afin d'obtenir l'autorisation de transférer des données personnelles de l'UE vers les États-Unis » : https://www.glossaire-international.com/pages/tous-les-termes/safe-harbor.html.

[480] Haas G., Goutorbe L., Invalidation du *Safe Harbor* par la CJUE : quelles sont les conséquences juridiques et opérationnelles pour les entreprises européennes transférant leurs données en vertu de ce dispositif ? A propos de JUE, 6 octobre 2015, Affaire C-362/14, 28 octobre 2015 : https://www.haas-avocats.com/ecommerce/invalidation-safe-harbor-par-cjue-quelles-sont-les-consequences-juridiques-operationnelles-pour-les-entreprises-europeennes-transferan« -leurs-donnees-vertu-dispositif/.

[481] Edward Snowden, Pendant que vous lisez ceci, le gouvernement en prend note, Libération, Tribunes, juin 2015. V. également, Deroudille A. et Fatah F., L'extraterritorialité du RGPD dans le contexte du « Cloud Act », Rev. UE 2019. n°442.

sanctionnée par un quelconque contrôle juridictionnel ni soumise à une quelconque condition de nécessité ou de proportionnalité »[482]. Cet accord était effectif et applicable jusqu'à ce que la Cour de justice de l'Union européenne le suspende dans une décision du 6 octobre 2015[483]. Dans cette décision, il a été considéré que « l'accès général et incontrôlé des autorités publiques américaines aux données des citoyens européens pour des raisons sécuritaires, accès dont l'ampleur a été révélée par Edward Snowden, viole, selon la Cour, les droits garantis par la Charte européenne des droits fondamentaux (art. 7, art. 8 et art. 47) »[484]. Également, la Cour a considéré que les États-Unis n'offrent pas un niveau de protection adéquat aux données personnelles transférées. Précisément, elle a jugé que « la législation permettant aux pouvoirs publics d'accéder de manière généralisée au contenu des communications électroniques doit être considérée comme compromettante pour l'essence même du droit fondamental au respect de la vie privée et qu'un État membre doit pouvoir vérifier si les transferts de données personnelles entre cet État et les États-Unis respectent les exigences de la directive européenne sur la protection des données personnelles »[485]. En définitive, cet accord a été invalidé par la CJUE sur le fondement du droit fondamental au respect de la vie privée et du droit à la protection des données à caractère personnel.

***225.*** À la suite de cette suspension, un nouvel accord devait être trouvé pour autoriser le transfert des données de l'Union européenne vers les États-Unis.

b) L'insuffisance du niveau de protection des données par l'accord du « EU-US. Privacy Shield »

***226.*** À la suite de la suspension par la CJUE de l'accord Safe Harbor, un nouvel accord a été trouvé entre l'Union européenne et les États-Unis le 12 juillet 2016 (entrée en vigueur le 1er août 2016), dénommé « EU-US. Privacy Shield » considéré comme permettant de garantir un niveau de protection essentiellement équivalent aux exigences européennes. Cet accord édictait les règles relatives à la collecte, l'utilisation et la conservation des informations

[482] Deroudille A. et Fatah F., L'extraterritorialité du RGPD dans le contexte du « Cloud Act », Rev. UE 2019. n°442.

[483] CJUE, gr. ch., 6 oct. 2015, aff. C-362/ 4, Maximillian Schrems c/ Data Protection Commissioner : Décision de la CJUE invalidant le Safe Harbor. V. Chassigneux, C.,Aterritorialité des atteintes face aux logiques territoriales de protection juridique et problème de l'absence d'homogénéité des législations protectrices (quid des safe harbor principles), Lex Electronica, vol. 9, n°2, Numéro Spécial, 2004.

[484] L'invalidation du Safe Harbor par la CJUE : tempête sur les transferts de données vers les États-Unis, La Semaine Juridique Edition Générale n° 46-47, 9 novembre 2015, 1258.

[485] Communiqué 'e Presse n°117/15, CJUE, 6 octobre 2015, arrêt dans l'affaire C-362/14 Presse et Information Maximillian Schrems / Data Protection Commissioner. V. également, Donnat F., Droit européen de l'internet : réseaux, données, services, Issy-les-Moulineaux, LGDJ, 2018, 207 p.

personnelles provenant des États membres de l'Union européenne (y compris les pays membres de l'EEE), du Royaume-Uni et de la Suisse[486]. En analysant cet accord, il apparaissait que le niveau de protection des données aux États-Unis était équivalent à celui de la réglementation européenne. Il a été mis en lumière que bien que comportant des règles protectrices dans le cadre de transfert des données, celles-ci étaient mises à mal par d'autres lois américaines de lutte contre le terrorisme notamment. À la suite de cet accord, plusieurs entreprises américaines, dont les sociétés Microsoft et Google ont été certifiées et ont disposé de ce fait le droit de transférer des données à caractère personnel de l'Union européenne vers les États-Unis. Cet accord « EU-US. Privacy Shield » à l'instar du *Safe Harbor*, a également été décrié, notamment par l'organisation Digital Rights d'Ireland, laquelle a formé un recours, le 19 septembre 2016, contre la décision d'adéquation adoptant le *Privacy Shield* devant la CJUE. Dans la décision numéro T-670/16 du 22 novembre 2017, le tribunal de l'Union européenne a déclaré irrecevable le recours en annulation formé par l'association[487]. Le tribunal ne s'est, donc, pas prononcé sur le fond et a considéré que « l'association n'a pas la qualité pour agir au nom de ses membres ou du public d'une manière générale et qu'elle ne peut pas non plus agir pour son propre compte puisqu'une personne morale n'est pas titulaire d'un droit à la protection des données personnelles »[488]. Dans le cadre d'un nouveau recours contre la décision d'adéquation adoptant le *Privacy Shield*, la CJUE a décidé, dans son arrêt en date du 16 juillet 2020[489], d'invalider la décision 2016/1250 relative à l'adéquation de la protection assurée par le Privacy Shield ou le bouclier de protection des données UE-États-Unis[490]. Cette invalidation a été confirmée dans un autre arrêt de la grande chambre de la CJUE en date du 6 octobre 2020[491] dans lequel il a été relevé, concernant la législation américaine, que des ingérences fondées sur des exigences relatives à la sécurité nationale dans les droits fondamentaux de la personne dont les données à caractère personnel pourraient être transférées depuis l'Union européenne vers les États-Unis peuvent notamment résulter de l'accès à ces données et de leur utilisation par les autorités publiques américaines « se référant à cet égard aux programmes de surveillance tels que PRISM

[486] Liste des décisions d'adéquation rendues par la Commission européenne : https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#dataprotectionincountriesoutsidetheeu.

[487] Ordonnance du Tribunal de l'Union européenne du 22 novembre 2017 – Digital Rights Ireland/Commis ion, Affaire T-670/16 publié au JO C 410 du 7.11.2016 : http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130dc6a96c9e4049349eb87428e418c33800e.e34KaxiLc3eQc40LaxqMbN4Pbh0Ne0?text=&docid=198664&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=1446444.

[488] Article de Villedieu A.-L. et de Benezeth B., publié sur le site LEXplicite : https://www.lexplicite.fr/privacy-shield-faut-il-que-tout-change-pour-que-tout-reste-comme-avant/.

[489] CJUE Data Protection Commissioner/Maximillian Schrems et Facebook Ireland du 16 juillet 2020, affaire C-311/18.

[490] Ibid.

[491] CJUE Privacy International contre Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service, 6 octobre 2020, affaire C-623-17.

(programme permettant à la NSA, au FBI et à la CIA d'avoir accès aux communications envoyées ou reçues par l'intermédiaire des fournisseurs de services internet), UPSTREAM (programme permettant à la NSA de contraindre les entreprises de télécommunications de copier et de filtrer les flux de trafics internet) ou à l'Executive Order 12333 (programme permettant à la NSA d'accéder aux câbles sous-marins de plancher de l'Atlantique et ainsi de collecter et conserver des données avant leur arrivée aux États-Unis) »[492]. Cette décision d'invalider le *Privacy Shield* est prise, également, sur le fondement du droit fondamental au respect de la vie privée et du droit à la protection des données à caractère personnel.

***227.*** Pour comprendre cette affaire dite Schrems 2[493], il faut avoir à l'esprit la précédente affaire lorsque, en 2013, Monsieur Schrems avait déposé une plainte contre les pratiques de transfert de données de Facebook auprès de l'autorité irlandaise de protection des données (Data Protection Commission ou DPC). Cette plainte avait abouti en 2015 à l'invalidation du cadre de Safe Harbor entre les États-Unis et l'Union européenne par la CJUE dans son arrêt du 6 octobre 2015[494] qui avait eu pour conséquence de priver des entreprises du cadre Safe Harbor. À la suite de cette invalidation, ces entreprises ont, donc, adopté des clauses contractuelles types pour continuer à transférer des données en dehors de l'Union européenne[495]. À la suite de la décision de la CJUE de 2015[496], Monsieur Schrems a déposé auprès du DPC (Data Protection Commission, il s'agit de l'autorité irlandaise de protection des données) une nouvelle plainte portant sur le transfert de données à caractère personnel par Facebook de l'Union européenne vers les États-Unis fondée, cette fois-ci, sur l'utilisation des clauses contractuelles types. À cette plainte contre l'utilisation des clauses contractuelles types, l'autorité irlandaise de protection des données (Data Protection Commission ou DPC) a demandé aux tribunaux des précisions quant à la validité du bouclier de protection et a déposé un recours auprès de la Haute Cour irlandaise, laquelle a décidé de renvoyer l'affaire à la CJUE avec 11 questions[497]. La demande de décision préjudicielle présentée par la Haute Cour d'Irlande concernait, ainsi, le mécanisme « des garanties appropriées » permettant de transférer des données à caractère personnel de l'Union

[492] Lapotre C., actualité jurisprudentielle en matière de données personnelles : La Cour de justice se pose en gardienne des droits fondamentaux des citoyens de l'Union européenne, publié dans la revue du journal du management juridique et réglementaire, n°79 novembre-décembre 2020.

[493] CJUE, 16 juillet 2020, affaire n° C-311/18, Data Protection Commissioner contre Maximillian Schrems et Facebook Ireland.

[494] CJUE, gr. ch., 6 oct. 2015, aff. C-362/ 4, Maximillian Schrems c/ Data Protection Commissioner : Décision de la CJUE invalidant le Safe Harbor.

[495] V. art. 47 du RGPD relatif aux règles d'entreprise contraignantes.

[496] CJUE, gr. ch., 6 oct. 2015, aff. C-362/ 4, Maximillian Schrems c/ Data Protection Commissioner : Décision de la CJUE invalidant le Safe Harbor.

[497] CJUE, gr. ch., 6 oct. 2015, aff. C-362/14, Maximillian Schrems c/ Data Protection Commissioner: Décision de la CJUE invalidant le Safe Harbor, en présence de The United States of America, Electronic Privacy Information Centre, BSA Business Software Alliance, Inc., Digitaleurope.

européenne vers un État tiers et plus particulièrement, sur la validité de la décision 2010/87/UE, par laquelle la Commission a établi des clauses contractuelles types pour certaines catégories de transferts, à la lumière des articles 7, 8 et 47 de la charte des droits fondamentaux de l'Union européenne. Dans cette affaire, il est rappelé dans l'avis de l'avocat général de la CJUE, « qu'en l'absence de garanties communes en matière de protection des données à caractère personnel au niveau mondial, les flux transfrontaliers de ces données comportent un risque de violation de la continuité du niveau de protection garanti dans l'Union européenne. Soucieuse de faciliter ces flux tout en limitant ce risque, le législateur de l'Union européenne a mis en place trois mécanismes permettant de transférer des données à caractère personnel de l'Union européenne vers un État tiers »[498]. Ces doutes mettaient indirectement en cause les appréciations faites par la Commission à cet égard dans la décision d'exécution 2016/1250 ». Le 9 juillet 2019, la CJUE a entendu les plaidoiries orales dans l'affaire puis le 19 décembre 2019, l'avocat général de la Cour de justice de l'Union européenne (CJUE), Henrik Saugmandsgaard ØE, a rendu son avis sur la validité des clauses contractuelles types (CSC) ; il en résultait dudit avis que « l'opinion rendue confirme que les entreprises qui s'appuient sur les CSC n'ont pas à envisager de modifier leur approche pour le moment »[499]. Dans cet avis, il était mis en lumière des questions de fond, à savoir, est-ce que le droit de l'UE s'applique lorsque les données à caractère personnel de la personne concernée sont traitées par des autorités publiques dans un pays tiers ?

[498] Concernant le rappel des mécanismes permettant les transferts par l'avocat général de la Cour de justice des Communautés européennes (CJCE), Henrik Saugmandsgaard ØE, « D'abord, un transfert des données en dehors de l'UE peut avoir lieu sur la base d'une décision par laquelle la Commission européenne estime que l'État tiers en question assure un « niveau de protection adéquat » des données qui lui sont transférées. Ensuite, en l'absence d'une telle décision, le transfert est autorisé lorsqu'il est accompagné de « garanties appropriées ». Ces garanties peuvent prendre la forme d'un contrat entre l'exportateur et l'importateur des données contenant des clauses types de protection adoptées par la Commission. Enfin, certaines dérogations, fondées notamment sur le consentement de la personne concernée, qui permettent le transfert des données vers un pays tiers, même en l'absence d'une décision d'adéquation ou de garanties appropriées. Dans cette affaire « la juridiction de renvoi a mis en évidence certains doutes relatifs, en substance, à l'adéquation du niveau de protection garanti par les États-Unis en ce qui concerne les interférences des services de renseignement américains dans l'exercice des droits fondamentaux des personnes dont les données sont transférées aux États-Unis » : Schrems 2.0 : Cour de justice des Communautés européennes L'avocat général end ses conclusions, CompleDiscovery, 20 décembre 2021 : https://complexdiscovery.com/schrems-2-0-european-court-of-justice-advocate-general-renders-opinion/?amazonai-language=fr) et https://curia.europa.eu/jcms/jcms/Jo1_6308/.

[499] Concernant les CSC, l'avocat général de la Cour de justice des Communautés européennes (CJCE), Henrik Saugmandsgaard ØE propose à ce que la Cour réponde « réponde comme suit aux questions préjudicielles posées par la Haute Cour d'Irlande : L'analyse des questions préjudicielles n'a révélé aucune incidence sur la validité de la décision 2010/87/UE de la Commission du 5 février 2010 relative à des clauses contractuelles types pour le transfert de données à caractère personnel à des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil, telle que modifiée par la décision d'exécution (UE) 2016/2297 de la Commission du 16 décembre 2016 ». Concernant les clauses contractuelles types, l'avocat général indique que « dans des cas particuliers celles-ci peuvent ne pas apporter de réponse aux problèmes qui se posent lorsque les transferts de données transmettent les données des citoyens de l'UE sous la responsabilité des autorités publiques américaines ». Par ailleurs, il est noté des questions de complexités procédurales telles « qui devrait intervenir lorsque, dans le cadre d'un transfert individuel, le niveau de protection exigé par le droit de l'UE ne peut être maintenu ». En l'espèce, « tout en reconnaissant ses imperfections et les difficultés pratiques qu'elle présente, et nonobstant le risque de fragmentation entre les autorités de contrôle au sein des États membres, l'avocat général conclut que l'approche adoptée par l'UE dans le cadre des clauses contractuelles types constitue un équilibre approprié entre pragmatisme et principe ». Enfin selon l'avocat général, la responsabilité de garantir la protection des droits des citoyens de l'UE en matière de protection des données incombe en premier lieu aux responsable du traitement et aux autorités nationales de contrôle lorsqu'un responsable du traitement ne s'acquitte pas de ses obligations : https://complexdiscovery.com/schrems-2-0-european-court-of-justice-advocate-general-renders-o'inion/?amazonai-language=fr.

Ensuite, est-ce que les lois et pratiques américaines facilitent les atteintes aux droits des personnes en matière de protection des données qui sont incompatibles avec le droit de l'UE ? À cette question, l'Avocat général répond que les autorités américaines le font. Enfin, est-ce que ces problèmes ont été résolus par le bouclier de protection des données ? À cette dernière question, l'avocat général répond par la négative[500]. Il en ressort de cet avis que le bouclier de protection des données ne permettait, donc, pas de garantir la protection des données des citoyens européens conformément au droit de l'Union européenne. Le Privacy Shield est considéré comme n'étant « plus un mécanisme valable lors du transfert de données personnelles de l'Union européenne vers les États-Unis. Toutefois, cette décision ne libère pas les participants au programme EU-U.S. Privacy Shield de leurs obligations au titre du cadre UE-U.S. Privacy Shield [501].

***228.*** S'agissant de l'utilisation des clauses contractuelles types par les entreprises, celles-ci n'ont pas été remises en cause dans cet avis et demeurent pleinement valables. Dans cette affaire SCHREMS 2, la CJUE reconnaît « la légalité des clauses contractuelles types, mais met à la charge des responsables et sous-traitants exportateurs de données, en collaboration avec l'importateur, l'obligation de vérifier que la législation ou la pratique du pays tiers n'empiète pas sur l'efficacité des garanties appropriées contenues dans ces clauses, ou le cas échéant, dans les outils visés à l'article 46 du RGPD »[502]. Il a, également, été rappelé par la CJUE dans le cadre de son communiqué de presse du 16 juillet que « la décision 2010/87 de la Commission relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers est valide »*[503]*. À la suite de la décision de la CJUE du 16 juillet 2020 invalidant le *Privacy Shield*[504], les acteurs comme Google, bénéficiant de ce régime de faveur, ont déclaré avoir revu leurs politiques de collecte et de traitement des données à la lumière du RGPD. Au vu de tous ces éléments démontrant l'hégémonie réglementaire des États-Unis, il apparaît que l'effectivité des règles de protection des données à caractère personnel, en matière de transfert des données consacrées par l'Union européenne, est remise en cause, soit par la primauté des lois sécuritaires américaines sur celles européennes, soit par

[500] Avis du 19 décembre 2019 de l'avocat général de la Cour de justice de l'Union européenne (CJUE) sur la validité des clauses contractuelles types (CSC).

[501] Recueil Dalloz, Schrems II et invalidation du Privacy Shield, un goût de « déjà vu », Céline Castets-Renard – D. 020. 2432.

[502] Eynard J. et Monteil M., Transferts de données : le CEPD revient sur les conséquences de l'arrêt Schrems II –Dalloz actualité 7 juillet 2021.

[503] CJUE, communiqué de presse n°91/20 du 16 juillet 2020, à la suite de la décision relative à l'invalidation du Privacy Shield (CJUE, 16 juillet 2020, affaire n° C-311/18, Data Protection Commissioner contre Maximillian schrems et Facebook Ireland) : https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091fr.pdf.

[504] CJUE Data Protection Commissioner contre Maximillian Schrems et Facebook Ireland, 16 juillet 2020, affaire C-311/18.

l'insuffisance de la protection des données dans le cadre des accords pour le transfert des données conclus entre l'Union européenne et les États-Unis.

***229. Des inquiétudes persistantes sur la protection des données avec l'adoption du cloud Act.*** Le Cloud Act a été adopté à la suite de la décision de la Cour suprême des États-Unis, dans l'affaire Microsoft. Dans cette affaire, le tribunal de New York avait délivré un mandat autorisant la police américaine à perquisitionner des données détenues dans les serveurs de la filiale européenne du groupe, située en Irlande[505]. À la suite de cette décision, la société Microsoft a soulevé l'inapplicabilité du mandat américain à des perquisitions menées hors du champ de compétence des juridictions américaines, sur le territoire de l'Union européenne[506]. L'affaire a été portée devant la Cour suprême qui a décidé, le 17 avril 2018, l'abandon des poursuites du 17 avril 2018[507]. C'est à la suite de cette décision qu'a été adopté le « Cloud Act », lequel suscite un risque « de conflit juridique avec les règles fixées par les articles 48 et 28 du RGPD » [508]. Ce texte « organise ainsi un accès sans limite (dès lors qu'il y a des soupçons de « serious crime », c'est-à-dire n'importe quelle infraction punie de plus d'un an d'emprisonnement...) des autorités judiciaires américaines aux données des personnes morales »[509]. Tel que rappelé par Monsieur Gauvain, « il ressort de l'article 48 précité qu'une décision d'une juridiction ou d'une autorité administrative d'un État tiers - tel qu'un mandat judiciaire exigé au titre du 4e amendement - ne suffit pas, par elle-même, à fonder légitimement la communication de données couvertes par le RGPD »[510]. À ce sujet, la Commission européenne a rappelé que la décision d'une juridiction ou d'une autorité administrative d'un État tiers doit se fonder sur une convention internationale, telle qu'un traité d'entraide judiciaire, et lui, soit conforme[511]. Dans ce contexte, la doctrine appréhende que le Cloud Act rende « obsolètes et inutiles les Traités d'entraide judiciaire. Il organise un système dans lequel seules les autorités judiciaires américaines bénéficient d'un accès quasi instantané à l'ensemble des données des personnes morales »[512].

---

[505] Deroudille A. et Fatah F., L'extraterritorialité du RGPD dans le contexte du « Cloud Act », Rev. UE 2019. n°442.

[506] Ibid.

[507] Cour suprême des États-Unis, per curiam, United States petitioner vs/ Microsoft Corporation ; 584 US (2018) ; n° 17-2.

[508] Deroudille A. et Fatah F., L'extraterritorialité du RGPD dans le contexte du « Cloud Act », Rev. UE 2019. n°442.

[509] Gauvain R., Rapport parlementaire sur les procédure[s] extraterritoriales, Revue Lamy droit des affaires, N° 157, 1er mars'2020.

[510] Ibid.

[511] Amicus curiae présenté par la Commission de l'Union européenne dans l'affaire Microsoft Ireland.

[512] Gauvain R., Rapport parlementaire sur les procédure[s] extraterritoriales, Revue Lamy droit des affaires, N° 157, 1[er] mars 2020.

***230.*** Pour tenter de remédier à l'extraterritorialité unilatérale du droit américain en matière de protection des données, un groupe d'experts[513] a préconisé les autorités françaises et européennes « d'étendre les dispositions du RGPD, lequel texte peut, à leur sens constituer un standard international en matière de protection des données personnelles »[514]. Également, il est proposé par la doctrine d'envisager « la conclusion d'un accord entre l'Union européenne et les États-Unis, qui fixerait avec beaucoup plus de précisions les conditions d'extraterritorialité réciproques des différentes mesures d'investigation, américaines et européennes que les accords actuels. Un tel procédé pourrait d'ailleurs avoir le mérite de faire bénéficier l'Union européenne de la qualité de « Qualifying foreign government », au sens du « Cloud Act », dont le droit peut faire obstacle à une divulgation exigée par l'administration américaine »[515].

***231.*** Après avoir constaté la prééminence théorique du droit européen de la protection des données sur les réglementations étrangères et notamment étasuniennes, il s'agit de poursuivre l'analyse par rapport, cette fois-ci, à l'étude du contrat de cloud computing.

## B) Une critique fondée sur le montage contractuel opéré par les fournisseurs de services cloud

***232.*** Cette partie repose sur l'étude du montage contractuel opéré par certains prestataires de services cloud, notamment américain, pour obtenir une certification de conformité à la réglementation générale de la protection des données de l'Union européenne. Il convient, tout d'abord, d'analyser la politique du transfert des données dans le cadre d'un contrat de cloud computing (1), puis d'étudier les clauses sensibles du contrat de cloud computing en matière de transfert des données (2).

### 1) L'analyse du montage contractuel pour l'obtention d'une autorisation de transfert des données

***233.*** La société Google collecte en masse les données de ses utilisateurs, personnes physiques, et les héberge dans des serveurs situés en dehors du pays de résidence de ces derniers. Il est, donc, envisagé d'étudier sa politique du transfert des données. En sa qualité de société américaine, la société Google est soumise aux pouvoirs d'enquête et d'exécution de la Commission Fédérale

[513] Bérard M.-H., Lamy P., Vimont P., Schweitzer L. et Fatah, F. L'Europe face aux sanctions américaines, quelle souveraineté ? *Policy Paper* n° 232, Institut Jacques Delors.

[514] Deroudille A. et Fatah F., L'extraterritorialité du RGPD dans le contexte du « Cloud Act », Rev. UE 2019. n°442.

[515] Ibid.

du Commerce américaine ou FTC (Federal Trade Commission) et à la réglementation sécuritaire des États-Unis, telle que « Cloud Act »[516]. En application de ces lois sécuritaires, le gouvernement américain a le droit d'exiger des prestataires de services cloud la communication des données des utilisateurs même si ces derniers sont des résidents de l'Union européenne.

***234.*** Pour opérer des services de cloud computing sur le territoire européen, Google a passé en revue ses processus et s'est conformée aux principes énoncés dans l'accord Privacy Shield concernant la collecte, l'utilisation et la conservation des informations personnelles provenant des États membres de l'Union européenne afin de pouvoir obtenir la certification aux principes de Privacy Shield, laquelle a été obtenue par Google et a disposé de ce fait le droit de transférer des données à caractère personnel de l'Union européenne vers les États-Unis. À la suite de l'invalidation du *Privacy Shield*, la question s'est posée de savoir quelle est la valeur de cette certification. La certification aux principes de Privacy Shield permettait d'identifier les responsables dans le cadre du traitement, de la collecte et du transfert des données. La société Google est considérée comme étant le responsable des informations personnelles qui vont être transmises à des tiers en vue d'un traitement externe. Cette responsabilité affirmée dans l'accord Privacy Shield était prise en application du principe relatif à ce type de transfert de données, dénommé « Onward Transfer Principle »[517]. Elle permettait, également, au titulaire de la certification (ici la société Google) du droit de transférer des données à caractère personnel de l'Union européenne vers les États-Unis. Aujourd'hui, l'accord EU-US Privacy Shield a été invalidé par la CJUE dans son arrêt du 16 juillet 2020[518]. À la suite de l'invalidation par la CJUE de l'accord EU-US Privacy Shield, Google a déclaré avoir revu sa politique de collecte et de traitement des données pour se conformer aux prescriptions du RGPD. En outre, la question s'est posée pour Google de savoir si elle pouvait continuer à transférer les données à caractère personnel de l'Union européenne vers les États-Unis. La réponse a été donnée par la CJUE, qui a considéré comme valide l'utilisation des clauses contractuelles types pour le transfert de données à caractère personnel hors de l'Union européenne[519]. Les entreprises ont, donc, adopté des clauses contractuelles types pour pouvoir poursuivre le transfert des données de l'Union européenne vers des pays tiers. En raison de l'utilisation de ces clauses contractuelles types approuvées par la Commission européenne dans les contrats cloud, elle a pu poursuivre les

[516] La « Federal Trade Commission » ou traduit par la « Commission Fédérale du Commerce américaine » a pour mission l'application du droit de la consommation et le contrôle des pratiques comme rciales anticoncurrentielles telles que les monopoles déloyaux://www.ftc.gov.

[517] Certifications officielles obtenues p r les entreprises américaines dans le cadre du Privacy Shield : https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI&status=Active.

[518] CJUE, 16 juillet 2020, affaire n° C-311/18, Data Protection Commissioner contre Maximillian Schrems et Facebook Ireland.

[519] CJUE, gr. ch., 6 oct. 2015, aff. C-362/14, Maximillian Schrems c/ Data Protection Commissioner : Décision de la CJUE invalidant le Safe Harbor.

transferts des données personnelles de ses clients, personnes physiques, de l'Union européenne vers les États-Unis.

***235.*** Concernant la valeur de ces clauses contractuelles types, la Commission a approuvé l'utilisation de ces clauses comme étant un moyen d'assurer une protection efficace dans le cadre d'un transfert de données en dehors de l'Union européenne. À l'instar de Google, la société Apple, pour être en conformité avec la réglementation européenne, utilise les clauses contractuelles types approuvées par la Commission européenne. Ces prestataires (tels que Google et Apple) intègrent dans les conditions d'utilisation du service cloud une disposition indiquant que tous les renseignements ainsi fournis sont susceptibles d'être transférés ou consultés par des entités du monde entier[520]. Cette clause a pour objet d'informer les clients, personnes physiques, que l'utilisation du service cloud implique l'acceptation au principe d'un transfert de leurs données à caractère personnel hors de l'Union européenne. En conséquence, les personnes physiques qui utilisent des services cloud fournis par des entreprises américaines consentent (de manière éclairée ou non) à ce que leurs données à caractère personnel soient transférées aux États-Unis. Une fois les données transférées dans ces serveurs, il est difficile, voire impossible, d'identifier de quelle manière et dans quel but seront utilisées les données. Ce flou quant à la détermination des utilisations projetées des données de résidents européens est amplifié par l'absence, au niveau fédéral des États-Unis, d'une réglementation générale à la protection des données à caractère personnel.

***236.*** Après avoir procédé à l'analyse du montage contractuel opéré par les prestataires de services pour obtenir une autorisation de transfert des données, il est question cette fois d'envisager l'étude des clauses sensibles du contrat de cloud computing en matière de transfert de données.

**2) L'analyse des clauses sensibles du contrat de cloud computing en matière de transfert des données**

***237.*** **Plan.** En matière de transfert des données, les clauses sensibles dans le contrat de cloud computing sont la clause relative au droit applicable (a) et à la localisation des serveurs pour l'hébergement des données (b).

[520] Politique du transfert des données d'Apple : « Dans ses conditions d'utilisation Apple informe que les données qui sont fournies dans le cadre de l'utilisation des services icloud peuvent être transférés par « des entités du monde entier » https://www.apple.com/legal/privacy/fr-ca/.

a) La clause relative au droit applicable

***238.*** La clause relative au droit applicable est présente dans tous les contrats, qu'il s'agisse des contrats conclus avec des personnes physiques ou des personnes morales. Elle a pour objet de déterminer le droit applicable au contrat. Dans les contrats conclus avec des consommateurs européens, le droit européen[521] rappelle à l'article 6.1 de la Directive européenne du 5 avril 1993[522] que « les États membres prennent les mesures nécessaires pour que le consommateur ne soit pas privé de la protection accordée par la présente directive du fait du choix du droit d'un pays tiers comme droit applicable au contrat, lorsque le contrat présente un lien étroit avec le territoire des États membres ». Cette disposition permet de protéger le consommateur contre l'application d'une clause ayant pour effet l'application du droit d'un pays tiers, lequel est moins protecteur. Cette protection du consommateur est matérialisée par la possibilité de déclarer la clause relative au droit applicable comme étant « abusive ». À titre illustratif, la CJUE[523] a considéré que la clause prévoyant l'application du droit luxembourgeois aux contrats entre Amazon et les consommateurs européens est abusive. En l'espèce, les conditions générales de ventes de la société Amazon contenaient une clause établissant l'application du droit de l'état membre dans lequel la société dispose son siège. Amazon avait établi son siège au Luxembourg. De ce fait, le droit luxembourgeois devait s'appliquer au contrat. L'association de protection des consommateurs établie en Autriche, *Verein für Konsumenteninformation*, considérait qu'une telle clause est abusive. La CJUE considère que « la loi de l'État membre du siège d'un professionnel régit le contrat conclu par voie de commerce électronique avec un consommateur est abusive pour autant qu'elle induise ce consommateur en erreur en lui donnant l'impression que seule la loi de cet État membre s'applique au contrat, sans l'informer du fait qu'il bénéficie également, en vertu de l'article 6, paragraphe 2, du règlement Rome I, de la protection que lui assurent les dispositions impératives du droit qui serait applicable en l'absence de cette clause ». En d'autres termes, pour que la clause désignant le droit luxembourgeois comme loi applicable au contrat soit considérée comme abusive, il faut que celle-ci engendre un déséquilibre significatif entre les droits et obligations des parties. Afin d'éviter qu'elle soit abusive, cette clause doit être rédigée de manière claire et compréhensible afin d'informer le consommateur de ses droits. Pour être valide, cette clause « ne doit pas donner l'impression au consommateur que seul le droit luxembourgeois est applicable au contrat, alors que le règlement "Rome I" dispose

[521] Directive n° 93/13/CEE du Conseil du 5 avril 1993, concernant les clauses abusives dans les contrats conclus avec les consommateurs. V. aussi Orientations de la Commission européenne relatives à l'interprétation et à l'application de la directive 93/13/CEE du Conseil concernant les clauses abusives dans les contrats conclus avec les consommateurs (JOUE C 323 du 27 sept. 2019).

[522] V. Directive européenne n° 93/13/CEE du 5 avril 1993, *op. cit.*.

[523] CJUE, 28 juill. 2016, affaire n° C-191/15, Verein für Konsumenteninformation c./ Amazon EU SARL.

clairement que le choix de la loi applicable ne peut pas avoir pour résultat de priver le consommateur de la protection que lui assurent les règles impératives de son pays de résidence soit les règles auxquelles il ne peut être dérogé par accord en vertu de la loi qui aurait été applicable en l'absence de choix »[524]. Il est rappelé que si cette information n'est pas communiquée au consommateur dans ce cas la clause est considérée comme étant abusive. La CJUE se prononce, également, concernant le droit applicable en présence d'un traitement des données personnelles. En l'espèce, Amazon effectue un traitement des données personnelles. La CJUE rappelle qu'au titre de la directive européenne sur le traitement des données[525] selon laquelle le droit applicable est la loi du pays où le responsable du traitement dispose d'un établissement et où ce traitement a lieu dans le cadre des activités de cet établissement. Le RGPD, ayant succédé à la Directive, il est précisé à l'article 3 du texte l'application du champ territorial du RGPD, lequel est plus élargi par rapport à celui de la Directive. À ce titre, le RGPD s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union, au traitement des données à caractère personnel relatif à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées à l'offre de biens ou de services ou au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union, au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union, mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public[526]. En conséquence dans un contrat de cloud conclu entre un professionnel et un consommateur prévoyant un traitement des données personnelles, la clause du droit applicable doit prévoir l'application du RGPD dès lors que l'on se trouve dans l'une des situations visées audit article 3.

***239.*** Compte tenu de ces règles, la question du droit applicable doit susciter une attention particulière des parties au contrat. Afin de limiter les risques au niveau contractuel, il est conseillé de prévoir une clause relative au droit applicable qui soumet le contrat cloud au respect du droit en vigueur de la réglementation européenne. En principe la rédaction d'une clause de droit applicable ne présente pas de difficulté rédactionnelle. À titre d'exemple, il est proposé, ci-après, une clause standard relative au droit applicable au contrat de cloud

[524] Revue Lamy Droit de l'Immatériel, Nº 129, Conditions générales de vente d'Amazon et clause de droit applicable abusive : précisions sur l'interprétation de règlements « Rome I » et « Rome II », 1er août 2016.

[525] Directive 95/46/CE 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[526] Art. 3 du RGPD.

computing « Le présent accord ainsi que ses annexes sont soumis à la réglementation française en vigueur ». En pratique, l'indication dans le contrat de cloud de computing d'une clause relative à l'application du droit de l'Union européenne, ne suffit pas à garantir l'inapplication de la réglementation américaine dès lors que le prestataire de services de cloud computing est une société américaine ou que les données sont stockées dans des serveurs situés aux États-Unis. En effet, un contrat peut avoir été formalisé sur le territoire de l'Union européenne entre une personne résidant sur ce même territoire et un prestataire de services cloud et malgré cela il y a un risque que les règles étasuniennes priment sur celles qui sont européennes. Dans cette configuration, la clause relative au droit applicable soumettant le cloud computing au respect de la réglementation est d'une efficacité limitée lorsque le prestataire de services cloud est une société américaine ou que les données sont hébergées dans des serveurs situés aux États-Unis.

b) La clause relative à la localisation des serveurs pour l'hébergement des données

***240.*** Outre la clause relative au droit applicable, la clause relative à la localisation des serveurs pour le stockage des données est une clause sensible. La doctrine met en lumière que « parmi les points particulièrement délicats, il faut citer en premier lieu le respect des dispositions protégeant les données personnelles. En effet, il est tout à fait possible que les données ou les applications du client se trouvent partiellement ou totalement stockées dans des centres informatiques (data centers) situés hors de l'Union européenne et dans des pays dont la législation n'accorde pas un niveau de protection suffisant »[527]. C'est pourquoi, en raison de cette insuffisance de protection, que certains auteurs sensibilisent les clients afin « d'obtenir du prestataire une information précise concernant la localisation de ses ressources en réseau et – au minimum – lui imposer une clause par laquelle il s'engage à assurer ses services depuis des centres qui soient situés dans l'Union européenne »[528]. À titre d'exemple, la société OVH affirme en annexe de ses conditions de services concernant la localisation et le transfert des données à caractère personnel que : « 6.1 Lorsque les Services permettent au Client de stocker des données, notamment des Données à caractère personnel, la ou les localisation(s), ou zone(s) géographique(s) du ou des centre(s) de zones géographiques sont disponibles, le Client sélectionne celle(s) de son choix au moment de la Commande. Sauf dérogation prévue dans les

[527] Warusfel B., sous la direction de Vivant M., le Lamydroit du numérique, Expert, Partie 3 Numérique et contrats Division 3 Les principaux contrats du numérique et leurs spécificités, Chapitre 6 Les contrats d'informatique dématérialisée (cloud computing), Section 2 Avantages et contraintes des prestations de cloud, Contraintes et risques des prestations de cloud, 22 avril 2022.

[528] Huet J. et Bouche N., Les contrats informatiques, LexisNexis, 2011, p. 81 ; V. également, Poggi A.-S. et Lefèvre A., Les offres Cloud pour entreprises et la protection des données à caractère personnel : les recommandations dont les entreprises doivent tenir compte lorsqu'elles choisissent une offre Cloud, RLDI 2014/106, no 3532, pp. 44-50.

conditions particulières de service en vigueur, OVH cloud s'interdit de modifier, sans l'accord du Client, la localisation ou la zone géographique prévue à la Commande »[529]. Dans ce sens, il n'y a pas d'interdiction à ce que le client puisse choisir le stockage de ses données dans des datacenters situés hors de l'Union européenne. Sur ce point, la société OVH précise que « 6.3 Concernant l'utilisation de Services localisés dans les centres de données non européens d'OVH cloud, (a) lesdits centres de données peuvent être situés dans des pays ne bénéficiant pas de décision d'adéquation de la Commission européenne dans les conditions prévues à l'article 45 du RGPD («Décision d'adéquation») et/ou (b) les données qui y sont stockées par le Client peuvent, conformément au paragraphe 6.2 ci-dessus et à l'article 7 ci-après, être traitées à distance depuis des pays ne bénéficiant pas de Décision d'Adéquation »[530]. La société OVH permet au client, personne physique, de choisir le lieu de la localisation du centre de données (datacenters) destiné à héberger les données du client.

***241.*** Dans le cadre d'un contrat de cloud computing, il faut accorder une vigilance toute particulière à la clause de localisation des données. Pour se prémunir contre une localisation des données hors des pays membres de l'Union européenne, il est envisageable de prévoir au niveau de la clause de localisation des données, une liste des pays hébergeant les serveurs du prestataire cloud ou une région ou le choix du client. Il est proposé, ci-après, une proposition de clause relative à l'engagement de la localisation des données dans des datacenters situés sur le territoire de l'Union européenne :

***242.*** « Le prestataire s'engage à stocker les données du client sur des serveurs localisés dans des pays situés sur le territoire de l'Union européenne, à communiquer au Client la localisation précise des serveurs dans lesquels sont stockées les données du client, à se conformer aux directives du Client quant au choix de la localisation des serveurs pour le stockage des données, à se conformer aux obligations issues de la législation du lieu de localisation des serveurs, à informer le client de tout incident pouvant avoir sur la localisation des serveurs pour le stockage des données du client ».

***243.*** En outre, l'effectivité d'une telle clause pourra être remise en cause si les États-Unis décident d'actionner les droits issus des lois sécuritaires, telles que le Patriot Act et le Cloud Act. Sur ce point, « le rapport Gauvain insiste sur les risques de portée extraterritoriale du Cloud Act pour les entreprises françaises qui confieraient leurs données au GAFAM »[531]. En effet, le gouvernement américain peut accéder aux données de toutes les personnes dès lors qu'elles sont

[529] Annexe traitement de données à caractère personnel ou "dpa" (version du 27 septembre 2021) aux conditions générales de service d'OVH (version du 6 mai 2022).

[530] Conditions particulières du service public CLOUD (version du 25 avril 2022).

[531] Augagneur L-M, Revue Lamy Droit de l'Immatériel (nº 162), Héberger ses données chez les GAFAM : quel discours croire sur le Cloud Act ? 1er août 2019.

stockées dans les serveurs d'une société américaine et de ses filiales européennes (situé aux États-Unis ou hors des États-Unis). En dépit d'une sécurisation des données par une clause contractuelle telle que par une clause de localisation des données, il y a toujours un risque que les États-Unis se saisissent des données de résidents européens. À ce titre, la doctrine propose d'intégrer une clause selon laquelle le prestataire de services (en l'espèce Microsoft) s'engage à « garantir qu'elle agirait systématiquement pour s'opposer à la communication des données, qu'elle en assumerait l'entière charge procédurale et les entières conséquences, y compris à l'égard du RGPD. Mais cette seule clause, à supposer qu'elle puisse être négociée, ne pourrait vraisemblablement pas trouver une efficacité absolue et n'empêcherait pas, en pratique, l'accès effectif aux données s'il était ordonné par les juridictions américaines »[532].

***244.*** En pratique, il apparaît, donc, que l'indication dans le contrat de cloud de computing d'une clause relative à la localisation des serveurs pour le stockage des données sur le territoire européen ne suffit pas à garantir l'inapplication de la réglementation américaine lorsque les données sont hébergées dans les serveurs d'une société américaine et de ses filiales européennes (situé aux États-Unis ou hors des États-Unis). En revanche, l'indication d'une clause de localisation des serveurs sur le territoire de l'Union européenne pour le stockage des données garde son utilité vis-à-vis des sociétés européennes lorsqu'elles s'engagent, d'une part, à stocker les données des utilisateurs dans des serveurs localisés en France ou en Union européenne et d'autre part, s'interdisent de les stocker et de transférer les données dans des serveurs localisés hors de l'Union européenne et en particulier aux États-Unis. Dans cette configuration, la clause dispose d'une utilité et permet de renforcer les droits et garanties de la personne physique par l'application de la réglementation protectrice de l'Union européenne.

[532] Ibid.

# Conclusion du chapitre 2

***245. L'existence d'un cadre légal européen du transfert des données.*** Au sein de l'Union européenne, chaque État membre est tenu au respect des mêmes règles de protection des données à caractère personnel. En matière de transfert de données au sein de l'Union européenne, le principe est la libre circulation des données. Concernant le transfert de données de l'Union européenne vers des pays tiers, le principe est la libre circulation sous réserve du respect de certaines conditions ayant pour objet de s'assurer du niveau de protection des données dans le pays tiers. Il n'y a, donc, pas une interdiction de principe au transfert de données hors de l'Union européenne, mais ce transfert doit s'inscrire dans le cadre défini par le RGPD. Malgré ce cadre, le transfert des données en dehors de l'Union européenne, notamment à destination des États-Unis, suscite des interrogations quant à la protection des données à caractère personnel.

***246. Les critiques de l'effectivité des règles européennes dans le cadre d'un transfert de données vers les États-Unis.*** L'adoption des lois sécuritaires et sa domination économique du marché des prestations de services cloud ont une incidence directe sur l'effectivité des règles européennes de protection des données à caractère personnel. Il apparaît une primauté des règles étasuniennes sur celles européennes. Ces lois sécuritaires affirment un droit d'accès et de collecte des données par les États-Unis et sont fondées sur des motifs de sécurité nationale. Outre l'hégémonie réglementaire, il a été démontré que l'effectivité des règles européennes de protection des données à caractère personnel est remise en cause en raison d'un montage contractuel opéré par les prestataires de services cloud étasuniens. Il a été envisagé d'analyser lesdites clauses comme celles concernant le droit applicable et à la localisation des serveurs. Il a été constaté que l'insertion de clauses contractuelles protectrices est d'une efficacité limitée lorsque le prestataire de services cloud est une société américaine ou que les données sont stockées dans des serveurs situés aux États-Unis. Il en résulte que dans le cadre d'une application de ces lois sécuritaires et en dépit d'une sécurisation contractuelle des données, il existe toujours un risque d'atteinte à la protection des données à caractère personnel des résidents européens, personnes physiques.

# Conclusion du titre 1

***247. La constatation de lacunes légales par l'application du régime général de la protection des données à caractère personnel dans les contrats de cloud computing.*** Dès lors que le contrat de cloud computing prévoit une licence de collecte et de traitement des données au profit du prestataire de services cloud, la réglementation relative à la protection des données à caractère personnel à vocation à s'appliquer et en particulier celle du RGPD. L'application du RGPD a été critiquée en raison que celle-ci n'est pas spécifique à l'usage de la technologie du cloud computing, mais est justifiée en raison de l'intégration d'une clause de collecte et de traitement des données dans les contrats de cloud computing. Des critiques ont été établies concernant l'intégration de cette clause, lesquelles sont fondées sur l'objet, la qualification du contrat et sur l'existence de déséquilibres contractuels.

***248. La constatation de lacunes légales en matière de transfert des données à caractère personnel hors de l'Union européenne.*** L'attention a été portée davantage sur la protection des données en matière de transferts de données de l'Union européenne vers des pays tiers. Il a été procédé à une analyse comparative entre le cadre réglementaire européen et étasunien. L'effectivité des règles de protection des données à caractère personnel est remise en cause face aux États-Unis en raison d'une part, de l'adoption de ces lois sécuritaires et d'autre part, par le montage contractuel opéré par les fournisseurs de services cloud. Les lois sécuritaires américaines ont une incidence directe quant à l'effectivité des règles européennes pour la protection des données en raison de la primauté des premières sur les secondes. L'inquiétude porte sur l'application des lois sécuritaires qui accordent un droit d'accès et de collecte des données des clients utilisant les services et ce peu importe si ces données concernent des personnes physiques résidant sur le territoire de l'Union européenne ou que ces données sont collectées depuis le territoire de l'Union européenne. Les règles européennes sont, également, remises en cause dans le cadre d'un montage contractuel. Certains prestataires de services cloud, notamment américains, ont travaillé « habilement » leur contrat de cloud computing afin d'obtenir « une certification de conformité » à la réglementation européenne. Pour autant, cette certification ne permet pas de s'assurer d'une protection effective des données dans les contrats de cloud computing. Face à ce montage contractuel et au risque d'atteinte au droit à la protection des données personnelles dans le cadre d'un contrat de cloud computing, il a été proposé d'accorder une attention particulière à la clause relative au droit applicable et à la clause relative à la localisation des serveurs pour le stockage des données. Malgré cette vigilance, il apparaît que l'intégration de ces clauses au contrat ne suffit pas à garantir

l'inapplication de la réglementation américaine dès lors que les données sont stockées dans les serveurs d'une société américaine et de ses filiales européennes (situées aux États-Unis ou hors des États-Unis).

# Titre 2 : Les lacunes légales de la protection des données des personnes morales dans les contrats de cloud computing

***249. L'identification du titulaire de la protection***. La personne morale est considérée comme un « groupement doté, sous certaines conditions, d'une personnalité juridique plus ou moins complète ; sujet de droit fictif qui, sous l'aptitude commune à être titulaire de droits et d'obligations, est soumis à un régime variable, notamment selon qu'il s'agit d'une personne morale de droit privé ou de droit public »[533]. En droit français, il existe deux catégories de personnes morales, celles de droit public (l'État, les collectivités territoriales et les établissements publics…) et celles de droit privé (les sociétés civiles, les sociétés commerciales, les groupements d'intérêt économique, les associations…)[534]. Tel qu'indiqué en introduction, l'attention est portée sur la protection des données des personnes morales de droit privé appartenant à la catégorie générique des données à caractère non personnel.

***250. La détermination des données à protéger***. Au niveau de sa terminologie, les données des personnes morales de droit privé correspondent aux informations relatives à son exploitation, ses finances, ses stratégies sur le marché, ses actions de marketing, ses portefeuilles clients et fournisseurs (volume de vente, prix, marge, identité des clients). La pratique définit les données stratégiques de l'entreprise comme étant « un ensemble d'informations qui si elles étaient détenues ou mises en corrélation par des tiers pourraient permettre de prendre de vitesse ou neutraliser une prise de position envisagée par l'entreprise et dont l'impact serait d'une telle ampleur, que la stratégie de l'entreprise serait fortement ou durablement impactée (..). Par ailleurs, le caractère stratégique d'une donnée est lié à la durée de validité de l'axe stratégique de l'entreprise (fusion, appel d'offres...). Une donnée stratégique peut alors être confidentielle ou sensible pendant un temps déterminé et perdre cette caractéristique ultérieurement »[535].

***251. L'exclusion du RGPD pour la protection des données des personnes morales***. Il est rappelé que dans le cadre d'un contrat de cloud computing conclu entre un client, personne morale, et un fournisseur de services cloud, le règlement général à la protection des données n'a pas vocation à s'appliquer aux données afférentes à la personne morale[536] puisqu'elles ne sont

[533] Suivant le dictionnaire vocabulaire juridique publié sous la direction de Gérard Cornu aux Presses universitaires de France. Également, la personne morale « désigne aussi, dans la théorie dite de la personnalité morale, la fiction en vertu de laquelle un groupement, un organisme, etc., est considéré comme un sujet de droit en soi, une entité distincte de la personne des membres qui le composent ».

[534] Campagne N., Du bon usage des règles « informatique et libertés » pour les fichiers d'entreprises, Revue Lamy Droit de l'Immatériel, 107, 01-08-2014.

[535] Définition du guide pratique cloud computing et la protection des données, CIGREF, IFACI, AFAI.

[536] Considérant 14 du RGPD.

pas considérées comme étant des données à caractère personnel. Il est expressément mentionné au considérant 14 du RGPD que « le présent règlement ne couvre pas le traitement des données à caractère personnel qui concerne les personnes morales, et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale ». Il n'existe pas pour l'heure une réglementation spécifique à la protection des données des personnes morales équivalente à celle applicable aux personnes physiques concernant la protection de leurs données personnelles. Il est question, alors, d'étudier les cadres légaux afin d'appréhender le niveau de protection des données des personnes morales et d'en observer ses applications dans les contrats de cloud computing.

***252. La protection légale des données des personnes morales par les droits de la personnalité***. L'intérêt pour la protection des données des personnes morales dans les contrats de cloud computing trouve sa source dans le constat que le développement des nouvelles technologies de l'information et de la communication a accru les atteintes aux données des personnes morales. Face à ce besoin de protection des données des personnes morales, certains auteurs ont milité pour la reconnaissance des droits dits de la personnalité au profit des personnes morales ; en particulier, le droit à la protection des données et le droit à la vie privée. Ils considèrent que l'application de ces droits à la personne morale permettrait de pallier l'existence d'un vide juridique relatif à la protection de leurs données. Cette proposition doctrinale est étudiée en vue d'apprécier si celle-ci peut effectivement renforcer la protection des données des personnes morales dans les contrats de cloud computing.

***253. La protection légale dans le cadre d'un transfert de données des personnes morales***. Les données des personnes morales sont considérées comme étant des données à caractère non personnel définies comme celles qui « englobent par défaut l'ensemble des données numériques qui n'entrent pas dans le champ des données personnelles telles que définies par le RGPD. Il peut s'agir de données commerciales, de données sur l'agriculture, de précision, sur les besoins d'entretien des machines, météorologiques, etc. »[537]. Au niveau européen, c'est le règlement européen dit RDNP du 14 novembre 2018[538] qui s'applique au transfert des données non personnelles. Celui-ci établit un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne[539]. Ce texte instaure un principe de libre circulation des données à caractère non personnel au sein de l'Union européenne qui sont qualifiées de

[537] Définition des données non personnelles : v. art. 4.1.1 du RDNP.

[538] Règlement (UE) numéro 2018/1807 du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne applicable depuis le 19 avril 2019. Ce texte a pour objet d'établir les règles en matière de transfert de données à caractère non personnel (celles qui ne concernent pas « une personne physique identifiée ou identifiable » et celles qui « étaient initialement des données à caractère personnel, mais qui ont ensuite été rendues anonymes ») et le principe consacré est la libre circulation des données au sein de l'Union européenne.

[539] V. art. 1er du RDNP.

« marchandises immatérielles »[540]. Il est envisagé d'étudier les conséquences de l'application du principe de libre circulation des données dans les contrats de cloud computing.

***254.*** **Plan du Titre 2 :** Cette partie a pour objet de mettre en lumière que la loi prise dans son acception large contient des lacunes quant à la protection des données des personnes morales (Chapitre 1) et que celles-ci sont perceptibles dans le cadre d'un transfert de données (Chapitre 2).

[540] Avis du Comité économique et social européen sur la « Communication de la Commission au Parlement européen et au Conseil — Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne », publié au Journal officiel de l'Union européenne, le 15 janvier 2020.

# Chapitre 1 : L'absence d'un régime général à la protection des données des personnes morales

***255. Le débat de l'application des droits de la personnalité à la personne morale***. Face au développement des nouvelles technologies de l'information, les atteintes au droit à la protection des données des personnes morales se sont accrues ces dernières années. Cette partie a pour objet d'appréhender le régime légal de protection des données des personnes morales. À ce titre, il est envisagé d'étudier le bénéfice des droits dits de la personnalité au bénéfice de la personne morale pour renforcer la protection de ses données dans le cadre de l'exécution d'un contrat de cloud computing. L'application au profit de la personne morale des droits de la personnalité a suscité un débat doctrinal. Il a été question de savoir, « si les personnes morales ont une personnalité au sens juridique du terme (la personnalité en tant qu'aptitude à être titulaire de droits), ont-elles pour autant une personnalité au sens où l'on entend ce terme dans l'expression "droits de la personnalité", c'est-à-dire une personnalité psychologique ou, peut-être plus justement concernant les personnes morales, une personnalité sociale ? »[541]. La doctrine est divisée concernant la consécration des droits de la personnalité au profit de la personne morale. Pour les opposants, l'argument principal avancé a été de considérer que la personne morale ne dispose pas de « dignité » laquelle est uniquement réservée à l'être humain tel que l'énonce l'article 16 du Code civil[542]. Dans ce sens, le professeur G. Loiseau a affirmé que « c'est l'être humain comme tel qui, par opposition à la chose, a une dignité motivant le respect. La considération de l'humanité en chacun détermine donc l'attribution des droits de la personnalité à tous en la circonscrivant aux seules personnes humaines »[543]. À cela s'ajoute l'argument de la « personnalité » et précisément « la personnalité psychologique », laquelle correspond à un double rapport de perception, « perception que l'individu a de son identité, perception que les autres ont de l'identité de cet individu »[544]. La personne morale est dépourvue d'une personnalité psychologique et ne peut donc prétendre au bénéfice des droits de la personnalité. Alors que pour la doctrine favorable à la consécration des droits de la personnalité, l'argument a été de considérer que : « si donc chaque personne physique a une personnalité très riche, puisqu'à la fois physique, psychologique ou sociale, qui lui est propre, il faut admettre que les personnes morales, si elles ont une personnalité beaucoup moins étendue, n'ayant pas de corps

[541] Lepage A., Répertoire du droit civil, Droits de la personnalité, n°165, septembre 2009, Dalloz (actualisation juin 2021).

[542] L'article 16 du Code civil énonce que « La loi assure la primauté de la personne, interdit toute atteinte à la dignité de celle-ci et garantit le respect de l'être humain dès le commencement de sa vie ».

[543] Loiseau G., des droits patrimoniaux de la personnalité en droit français, McGill Law Journal 1997, p. 319.

[544] Luciani A.-M., Les droits de la personnalité. Du droit interne au droit international, thèse, Paris I, 1996.

physique, n'en ont pas moins une personnalité psychologique et surtout sociale qui, à ce titre, mérite une protection »[545]. Il s'agirait, ici, d'admettre que la personne morale dispose « une personnalité sociale » afin de lui attribuer des droits de la personnalité[546]. Le professeur Kayser considère, à ce titre, qu'elle est « comme une réalité, qui est cependant différente de la personnalité juridique des personnes humaines. Les personnes morales sont, donc, investies de droits analogues aux droits de la personnalité. Elles sont seulement privées de ceux de ces droits dont l'existence a un lien nécessaire avec la personnalité humaine »[547]. En pratique, cette position n'est pas majoritairement retenue ; en revanche, des « traces » de celle-ci seront retenues dans la jurisprudence[548].

***256. La singularité du droit à la protection des données et du droit à la vie privée.*** Outre le débat sans fin de savoir si les personnes morales ont une personnalité au sens juridique du terme pour bénéficier des droits de la personnalité, il est envisagé d'étudier l'application du droit à la protection des données et le droit à la vie privée au profit de la personne morale, lesquels sont deux droits fondamentaux distincts et ne doivent pas être confondus[549].

***257.*** **Plan.** Il est envisagé, tout d'abord, d'étudier l'application des droits fondamentaux au bénéfice des personnes morales pour la protection de leurs données dans le cadre d'un contrat de cloud computing (Section 1) ; puis, d'envisager les effets de l'absence d'une réglementation spécifique pour la protection des données des personnes morales dans les contrats de cloud computing (Section 2).

[545] Mestre J., La protection, indépendante du droit de réponse, des personnes physiques et des personnes morales contre l'altération de leur personnalité aux yeux du public, JCP 1974. I. 2623, spéc. nº 4

[546] Lepage A., Répertoire du droit civil, Droits de la personnalité, n°165, septembre 2009, Dalloz (actualisation juin 2021).

[547] Kayser P., Les droits de la personnalité. Aspects théoriques et pratiques, RTD civ. 1971. 445, spéc. nº 35.

[548] Ibid.

[549] V. *supra* n° 98 concernant la distinction entre le droit à la vie privée et le droit à la protection des données à caractère personnel. V. également, Basdevant A. et Mignard JP., l'empire des données - essai sur la société, les algorithmes et la loi, Don Quichotte éditions, mars 2018, p.173.

## Section 1 : L'inapplication des droits fondamentaux à la personne morale

***258.*** L'étude des droits fondamentaux au profit de la personne morale porte précisément sur le droit à la protection des données et le droit à la vie privée. L'application des droits fondamentaux au profit de la personne morale a pour objectif de renforcer la protection des données des personnes morales dans le cadre des contrats de cloud computing. Il apparaît que le droit à la protection des données personnelles et le droit à la vie privée se distinguent en raison de leur nature et leur fonction singulières. Le droit à la protection des données vise « une protection a priori qui veille à empêcher la survenance d'un événement par le respect des conditions de licéité d'un traitement - consentement éclairé, usage légitime pour une finalité déterminée (…). Au contraire, le droit au respect de la vie privée constitue l'intrusion de la part des tiers ». Malgré cette distinction de nature, il n'en demeure pas moins qu'en pratique ces deux droits tendent à un rapprochement perceptible dans l'étude de la jurisprudence. En raison de cette distinction de nature et fonctionnelle, il est fait le choix de les analyser dans deux sous parties distinctes.

***259.*** **Plan**. Dans une première partie, il est envisagé d'étudier l'absence d'un droit fondamental à la protection des données (A) et dans une seconde partie, l'absence d'un droit fondamental à la vie privée (B).

### A) L'absence d'un droit fondamental à la protection des données personnelles

***260.*** **Plan**. Dans le cadre de cette étude, il est observé que les juges refusent de reconnaître au profit de la personne morale un droit fondamental à la protection des données des personnes morales (1) ; en revanche, les parties ne sont pas empêchées d'insérer dans le contrat cloud les déclinaisons du droit fondamental à la protection des données personnelles (2).

**1) Le refus par les juges de la reconnaissance d'un droit fondamental à la protection des données des personnes morales**

***261. Le périmètre du droit fondamental à la protection des données***. Le droit fondamental à la protection des données personnelles est consacré par les textes[550]. La question est de savoir si ce droit accordé aux personnes physiques peut être étendu au profit de la personne morale. Tout d'abord, le considérant 1 du RGPD précise que « la protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental ». Cet article est rédigé en des termes non équivoques, le droit fondamental consacré par cet article ne s'applique qu'au profit des personnes physiques. Ensuite, l'article 16, paragraphe 1 du Traité sur le fonctionnement de l'Union européenne et l'article 8 de la Charte des droits fondamentaux de l'Union européenne énoncent que « toute personne a droit à la protection des données à caractère personnel la concernant ». Cette disposition vise « toute personne » ; nous pouvons, donc, légitimement penser que ce terme englobe toutes les personnes qu'elles soient physiques ou morales. Il s'agirait, ici, d'appliquer l'adage « ubi lex non distinguit, nec nos distinguere debemus » principe selon lequel « là où la loi ne distingue pas, il n'y a pas lieu de distinguer ». Or, les juges vont adopter une position restrictive de l'application des droits fondamentaux aux personnes morales et notamment le droit à la protection des données personnelles.

***262. Le refus par les juges de la reconnaissance d'un droit fondamental à la protection des données des personnes morales***. Concernant l'appréciation de la gravité de l'atteinte au droit à la protection des données à caractère personnel, la CJUE a, dans un arrêt du 9 novembre 2010[551], distingué selon qu'il s'agissait de personnes morales ou de personnes physiques et en particulier lorsque le nom de la personne morale identifie des personnes physiques[552]. Dans cette affaire, il était contesté le contenu d'une publication sur un site internet relative aux bénéficiaires de fonds européens agricoles ; celle-ci diffusait au public les informations suivantes : « le prénom et le nom, lorsque les bénéficiaires sont des personnes physiques; le nom légal complet tel qu'il a été enregistré, lorsque les bénéficiaires sont des personnes morales ; le nom complet de l'association telle qu'il a été enregistré ou officiellement reconnue, lorsque les bénéficiaires sont des associations de personnes physiques ou morales sans personnalité

[550] V. art. 8 paragraphe 1 de la Charte des Droit Fondamentaux de l'Union Européenne et art. 16 paragraphe 1 du Traité sur le fonctionnement de l'Union Européenne.

[551] CJUE (grande chambre) du 9 novembre 2010, affaire n° C-92/09, Volker und Markus Schecke GbR et Hartmut Eifert et affaire n°C-93/09 contre Land Hessen : Protection des personnes physiques à l'égard du traitement des données à caractère personnel, validité de la publication des informations relatives aux bénéficiaires d'aides agricoles et fixant les modalités de celle-ci au regard des dispositions du droit de l'Union ( art. 7 et 8 de la Charte des droits fondamentaux de l'Union européenne et interprétation des articles 18 et 20 de la Directive 95/46/CE), affaires jointes. : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:62009CJ0092&from=fr.

[552] Campagne N, La protection « informatique et libertés » des données des personnes morales en Europe, Revue Le Lamy Droit de l'immatériel, n° 104, 1er mai 2014.

juridique propre; la municipalité dans laquelle le bénéficiaire réside ou est enregistré et, le cas échéant, le code postal ou la partie de ce code qui indique la municipalité (…) ». Dans cette affaire, la CJUE a indiqué qu'« il doit être rappelé en premier lieu que la publication imposée par l'article 44 bis du règlement numéro 1290/2005 et le règlement nº 259/2008 mettant en œuvre cet article, identifie nommément l'ensemble des bénéficiaires d'aides du FEAGA et du FEADER, parmi lesquels figurent à la fois des personnes physiques et morales. Or (…) les personnes morales ne peuvent se prévaloir de la protection des articles 7 et 8 de la charte à l'égard d'une telle identification que dans la mesure où le nom légal de la personne morale identifie une ou plusieurs personnes physiques ». Il est considéré, alors, que le droit fondamental à la protection des données ne s'applique pas aux personnes morales, mais est réservé uniquement aux personnes physiques identifiées. Concernant l'étude de l'application d'un droit fondamental à la protection des données des personnes morales, la CJUE a, dans son arrêt du 10 décembre 2020, opéré une distinction entre les données afférentes aux personnes morales et les données à caractère personnel et a considéré que « seules ces dernières (les données à caractère personnel) sont protégées en droit de l'Union, notamment par un droit fondamental dont ne peuvent dès lors bénéficier les personnes morales »[553]. Il en résulte que le droit fondamental à la protection des données ne s'applique pas aux personnes morales, mais est réservé uniquement aux personnes physiques.

***263. Une position jurisprudentielle critiquable***. Certains auteurs ont critiqué cette position jurisprudentielle en estimant que si « l'intitulé même du RGPD réserve cette protection aux personnes physiques, l'article 8 de la charte des droits fondamentaux la reconnaît à "toute personne", sans distinction aucune »[554]. Dans ce contexte, il s'est posé la question de savoir si les juges de la CJUE n'auraient pas outrepassé leurs rôles en restreignant le champ d'application

[553] CJUE, 10 déc. 2020, affaire n° C-620/19, Land Nordrhein-Westfalen c. D.H.T *:* « Au cas d'espèce, l'administration fiscale allemande a opposé un refus à D.H.T, le syndic de faillite d'une société de droit allemand, après qu'il a demandé, sur le fondement de la loi qui ouvre un accès aux informations officielles détenues par certains organismes, la communication de diverses données sur cette société pour évaluer l'opportunité d'actions révocatoires dans le cadre d'une procédure d'insolvabilité. D.H.T a saisi le tribunal administratif de ce refus. Après que ce dernier a largement fait droit à la demande, un appel fut interjeté en vain puis un pourvoi en Révision introduit devant la Cour administrative fédérale qui sursit à statuer pour saisir la Cour de justice d'une question préjudicielle. Celle-ci a trait au RGPD dès lors que le droit allemand l'a rendu directement et inconditionnellement applicable aux personnes morales (Art. 2a, § 5, 2º, du Code des impôts allemand.). Il s'agit d'évaluer la conformité d'une imitation du droit d'accès, permise en principe par l'article 23.1 RGPD, lorsqu'elle se justifie par la protection d'un intérêt financier important d'un État membre dans le domaine fiscal, et plus précisément par une opposition à des actions révocatoires susceptibles d'être mise en œuvre dans le cadre d'une procédure collective. La Cour de justice n'y répondra en raison de son incompétence. Bien que dans l'intérêt d'une interprétation uniforme du droit de l'Union, elle accepte, de façon constante, de se reconnaître compétente pour interpréter les dispositions du droit de l'Union rendues applicables par le droit national d'un État membre à des situations en principe exclues de son champ d'application (CJCE, 18 oct. 1990, affaire n° C-297/88 et C-197/89, Dodzi), tel n'était pas ce qui ressortait du code des impôts allemand. La Cour estime que ce dernier modifie « l'objet et la portée » du RGPD, quand l'article 23.1 du RGPD est lui spécifique à la protection des droits fondamentaux des personnes physiques. Elle conclut à l'absence d'intérêt manifeste à l'interprétation de ce texte puisque l'uniformité du droit de l'Union n'est pas en cause ».

[554] Pailler L., Pas de droit fondamental à la protection des données pour les personnes morales, Revue Lamy Droit de l'Immatériel, Nº 177, 1er janvier 2021.

de l'article 8 de la CEDH pourtant large[555]; puisque la protection est offerte à « toute personne » sans distinction. Dans l'arrêt de la CJUE en date du 10 décembre 2020, les juges ont refusé d'octroyer aux personnes morales le droit fondamental à la protection des données consacré à l'article 8 de la CEDH en se fondant sur l'article 1er du RGPD qui exclut les données des personnes morales du champ d'application[556]. Il est observé qu'en fondant sa décision sur la lettre de cet article, la CJUE renforce sa position pour légitimer sa décision relative au refus d'appliquer, au profit de la personne morale, le droit à la protection des données.

***264.*** La question de savoir si la personne morale dispose d'un droit fondamental à la protection des données n'est pas récente ; elle se posait, déjà, à la suite de la transposition de la directive 95/46 « données personnelles et société de l'information ». Dans le rapport au Premier ministre, G. Braibant s'était interrogé sur « l'extension aux personnes morales de la protection des informations nominatives » et il a distingué « qu'en France (…) le législateur a préféré y renoncer, parce que les enjeux sont différents : vie privée et liberté individuelle d'un côté, et secret des affaires de l'autre »[557]. Il en résulterait de cette position que la vie privée et la liberté individuelle seraient réservées uniquement à la personne physique et que la personne morale ne pourrait prétendre qu'au secret des affaires.

***265.*** Si le droit fondamental à la protection des données est refusé au profit des personnes morales, qu'en est-il concernant les déclinaisons du droit fondamental à la protection des données, tels que le droit à l'information[558], le droit d'accès aux données[559], le droit de rectification[560], du droit à l'effacement ou « droit à l'oubli»[561], le droit à la limitation du traitement[562], le droit d'opposition[563], le droit à la portabilité des données[564].

---

[555] Rôles de la CJUE : Veiller à ce que la législation de l'UE soit interprétée et appliquée de la même manière dans tous les pays de l'UE ; garantir que les pays et les institutions de l'UE respectent la législation européenne : https ://europa.eu/european-union/about-eu/institutions-bodies/court-justice_fr.

[556] Considérant 14 du RGPD « ne couvre pas le traitement des données à caractère personnel qui concernant les personnes morales ».

[557] Braibant G., Rapport Données personnelles et société de l'information. Transposition en droit français de la directive numéro 95/46, La documentation française, coll. « rapports officiels », 1998, p. 7.

[558] V. art. 13 du RGPD relatif à la liste des informations à fournir au client lorsque des données à caractère personnel sont collectées auprès de la personne concernée et art. 14 du RGPD relatif aux informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée.

[559] V. art. 15 du RGPD concernant le droit d'accès aux données à caractère personne et au droit d'obtenir une copie.

[560] V. art. 16 du RGPD relatif au droit de rectification des données à caractère personnel.

[561] V. art. 17 du RGPD concernant le droit à l'effacement des données ou le droit à « l'oubli ».

[562] V. art. 18 du RGPD relatif au droit à la limitation du traitement des données à caractère personnel.

[563] V. art. 21 du RGPD, il s'agit du droit pour la personne concernée de s'opposer à tout moment à un traitement de ses données à caractère personnel.

[564] V. art. 20 du RGPD, il s'agit du droit pour la personne physique d'exiger de recevoir du responsable du traitement ses données dans un format adapté et structuré lui permettant de faciliter leurs transmissions à un autre responsable du traitement.

**2) L'admission par convention des déclinaisons du droit fondamental à la protection des données**

***266.*** Il apparaît que si les personnes morales sont soumises au respect du RGPD lorsqu'elles collectent et traitent les données personnelles de leurs clients, elles ne peuvent prétendre à bénéficier des droits attachés à la protection des données à caractère personnel et garantis par ce texte. Cette exclusion, par l'article 4 du RGPD, est critiquable en raison des informations permettant de les identifier, telles que la dénomination sociale, le siège social, la nationalité, récépissé Kbis. Certains auteurs ont établi le constat que « ce déséquilibre entre les charges assumées par les sociétés pour la protection des données personnelles et les contreparties qui leur sont accordées n'est, selon nous, pas satisfaisant »[565]. En effet, dans un contexte d'accélération du développement des technologies informatiques et de croissance mondiale du flux des données, il paraît opportun de permettre à la personne morale de bénéficier d'une protection de ses données. Il s'agirait, en l'espèce, de lui accorder la faculté de contrôler l'utilisation de ses données et de bénéficier des droits quasi analogue à ceux défendus par le RGPD : un droit d'information, un droit d'accès, un droit à la portabilité (..).

***267.*** ***Le droit d'accès des personnes morales***. Historiquement, concernant le droit d'accès, la loi nº 78-17 du 6 janvier 1978 « relative à l'informatique, aux fichiers et aux libertés » a consacré dans son article 34, le droit pour toute personne d'avoir accès aux données à caractère personnel détenues par des organismes privés ou publics[566]. L'article 2 modifiée de cette loi précise que : « la personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement ». Se pose, ainsi, la question de ce qu'il faut entendre par « toute personne ». Autrement dit, est-ce que la personne morale bénéficie de ce droit d'accès aux données[567] ? Cette question a reçu une réponse négative, lors de la discussion parlementaire de la loi de 1978, en considérant que « cette loi s'inscrit dans la reconnaissance de nouveaux droits de l'Homme et tend à protéger la vie privée et les libertés publiques des seuls individus »[568]. Dans ce contexte, la CNIL, dans son deuxième rapport d'activité, se demandait « s'il n'existait pas un "droit de savoir" au nom des personnes morales »[569]. Elle va considérer que « si le droit d'accès établi par l'article 34 de la loi du 6 janvier 1978 a un caractère strictement individuel, il convient d'en reconnaître l'exercice aux

[565] Lacroix-De Sousa S., *Les sociétés face au RGPD : les enjeux de la compliance*, Revue des sociétés 2021, nº 6, p. 351.

[566] V. art. 34 et 36 de la loi du 6 janvier 1978 publiée au Journal officiel du 7 janvier 1978.

[567] Le professeur Frayssinet J. s'interrogeait sur ce qu'il fallait entendre par « toute personne » ; est-ce que le droit d'accès bénéficiait-il aux personnes morales comme aux personnes physiques ? D. 1984, jurispr., p. 587, note Frayssinet J.

[568] Campagne N., Du bon usage des règles « informatique et libertés » pour les fichiers d'entreprises, Revue Le Lamy Droit de l'immatériel, Nº 107, 1er août 2014.

[569] Ibid.

personnes physiques, représentants légaux des entreprises, dès lors que le nom de ces personnes figure dans le fichier en tant que dirigeant, actionnaire ou associé (…) que la diversification des sources d'informations du fichier en rend la mise à jour particulièrement malaisée ; que pour remédier à cet inconvénient, il y a lieu de garantir l'exercice le plus large du droit d'accès et de rectification ; qu'afin de faciliter l'exercice de ces droits, les mairies doivent, non seulement, assurer une publicité à l'acte réglementaire portant création du traitement, mais encore informer chaque entreprise de l'existence du fichier et des possibilités d'obtenir communication des informations qu'il contient »[570]. Par cette déclaration, la CNIL se positionne, ainsi, en faveur d'une protection large des données en conférant aux personnes morales un droit d'accès et de rectification lorsque les conditions sont remplies. Par la suite, certains auteurs s'interrogeaient sur la question de savoir si le droit d'accès s'exercera sur la totalité des données concernant l'entreprise ou seulement sur les données relatives à l'individu demandeur[571]. Sur ce point, le professeur J. Frayssinet considère que « les données non nominatives concernant les entreprises deviennent indirectement nominatives quand on peut, dans un même fichier, les rapprocher des renseignements nominatifs portant sur les représentants légaux »[572]. S'agissant de la mise en œuvre de ce droit d'accès, la CNIL précise que « les personnes morales n'ont pas directement accès aux fichiers, l'accès étant réservé aux seuls dirigeants s'ils figurent dans le fichier »[573]. La personne morale n'ayant pas de réalité physique, le droit d'accès aux données s'exerce par l'intermédiaire de ses représentants légaux. En outre, cet accès était conditionné à la présence de données nominatives des dirigeants ; ce qui signifiait que les données des personnes morales en étaient exclues. Il en résulte que l'admission du droit d'accès au profit uniquement des représentants légaux de la personne morale en présence de données nominatives revient à confirmer l'exclusion d'un droit d'accès pour la protection des données des personnes morales.

***268.*** La loi n° 2004-801 du 6 août 2004 est venue mettre un terme au débat sur la question de savoir si une personne morale pouvait exercer un droit d'accès[574] en modifiant les articles 39 et

[570] CNIL, délibération n° 84-28 du 3 juillet 1984 relative à la mise en œuvre par les mairies d'Arcueil, de Gentilly, d'Ivry-sur-Seine, de Villejuif et de Vitry-sur-Seine, d'un fichier d'entreprises.

[571] Campagne N., Du bon usage des règles « informatique et libertés » pour les fichiers d'entreprises, revue Lamy Droit de l'Immatériel, n°107, 01-08-2014.

[572] D. 1984, jurispr., p. 587, note Frayssinet J.

[573] Cnil, 6e Rapport d'activité du 1er janvier au 31 décembre 1985, Doc. fr., p. 37 (droit d'accès sur des informations sur une entreprise ; également, elle rappelle que « l'article 34 de la loi du 6 janvier 1978 accorde un droit d'accès à toute personne désireuse de savoir si un traitement automatisé porte « sur les informations nominatives la concernant » et que l'article 4 de ladite loi définit comme nominatives « les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent ».

[574] Campagne N., Du bon usage des règles « informatique et libertés » pour les fichiers d'entreprises, revue Lamy Droit de l'Immatériel, n°107, 01-08-2014.

suivants de la loi nº 78-17 du 6 janvier 1978[575] lesquels confèrent, dorénavant, explicitement un droit d'accès des représentants légaux concernant les données nominatives. Par la suite, ce droit d'accès réservé aux représentants légaux a été confirmé par la CNIL dans ses délibérations[576]. Il permet aux représentants légaux des personnes morales de vérifier les données nominatives les concernant et en cas d'erreur d'exiger une rectification, voire une suppression des données[577]. En revanche, ce droit d'accès des représentants légaux ne concerne que les données à caractère personnel de ces derniers et ne vise pas les données de la personne morale.

***269.*** En conséquence, il n'existe pas un droit d'accès aux données des personnes morales d'ordre légal. En revanche, les parties pourront prévoir dans le contrat cloud l'existence d'un droit d'accès d'ordre conventionnel. Il s'agira de prévoir une clause relative au droit d'accès de la personne morale par l'intermédiaire de ses représentants. Par cette clause, les représentants de la personne morale disposeront d'un droit d'accès et détiendront, ainsi, le monopole de l'accessibilité des données stockées dans le cloud. En principe, ce droit d'accès conventionnel est rattaché à une obligation à la charge du client (personne morale), celle de sécuriser les accès à son cloud, notamment par la mise en place d'une procédure sécurisée des mots de passe et des identifications. À titre d'exemple, le contrat cloud d'OVH précise que : « le Client est seul responsable de l'utilisation qu'il fait des Services, et notamment de la gestion des clés lui permettant de gérer ses habilitations et ses accès au Service, l'utilisation des Applications API, logiciels et outils mis à sa disposition par OVH, l'administration de ses abonnements et la gestion des données qu'il utilise dans le cadre des Services. Le Client doit posséder les compétences et connaissances techniques nécessaires et prendre connaissance des caractéristiques des Services avant de les utiliser »[578]. Il en résulte, ici, que la carence légale d'un droit d'accès aux données des personnes morales est compensée par l'existence d'un droit d'accès conventionnel. Des propositions rédactionnelles de la clause relative au droit d'accès seront réalisées dans la section ci-après.

---

[575] Précision concernant l'exercice du droit d'accès, article 39 : « Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ».

[576] Délibération de la Cnil nº 2009-498 du 17 septembre 2009 autorisant les nouvelles modalités de mise en œuvre du fichier bancaire des entreprises (Fiben) de la Banque de France concernant le droit d'accès : « Les personnes physiques ou les représentants légaux des personnes morales peuvent obtenir communication, sur place ou par écrit, de l'ensemble des informations enregistrées dans leur dossier en s'adressant, à Paris, à la direction des entreprises de la Banque de France ou, en région, à l'une de ses unités ou, dans les départements d'outre-mer, à une agence de l'IEDOM. (...) Les mêmes personnes peuvent également exercer le droit de rectification dans les mêmes conditions. Cependant, si les données contestées proviennent d'un établissement ou organisme déclarant, seul ce dernier peut procéder aux rectifications nécessaires ».

[577] Campagne N., Du bon usage des règles « informatique et libertés » pour les fichiers d'entreprises, revue Lamy Droit de l'Immatériel, n°107, 01-08-2014.

[578] Conditions particulières du service public Cloud (version du 25 avril 2022).

***270. Le droit à l'information***. De la même manière que pour le droit d'accès, le droit à l'information des personnes morales n'est pas prévu par la loi. Cette lacune légale est compensée par l'ingénierie contractuelle en prévoyant d'intégrer ce droit à l'information dans le contrat de cloud computing. À l'effet de rendre effectif ce droit à l'information, il est prévu une clause dont l'objet est de mettre à la charge du prestataire de services cloud une obligation générale de « conseil, d'information et de mise en garde »[579]. Outre cette obligation générale d'information, il est prévu des clauses d'information spécifiques telles que la clause relative à l'information du client « sur les différents lieux de stockage de données et de tous les traitements des données effectués dans le cadre de la prestation fournie »[580]. À titre d'exemple, la société OVH précise dans ses conditions générales de service que « concernant ses Services en cours d'utilisation, le Client est informé par courrier électronique et via son interface de gestion de toute évolution substantielle de nature à dégrader lesdits Services, au moins trente (30) jours calendaires avant la mise en œuvre de l'évolution »[581]. Il est ajouté, s'agissant de la gestion des incidents, que « OVH cloud s'engage à tenir le Client informé de l'état d'avancement des opérations. Si OVH cloud constate que ses Services sont disponibles et en bon état de fonctionnement, que l'existence de l'incident ne peut être confirmée ou que l'incident ne relève pas de la responsabilité d'OVH cloud, OVH cloud en informe le Client »[582]. Ces clauses permettent d'encadrer le périmètre des obligations d'information spéciales à la charge du Prestataire. En intégrant ces clauses dans le contrat de cloud computing, le client, personne morale, est titulaire conventionnellement d'un droit à l'information concernant la gestion et la sécurisation de ces données dans le cloud. À l'instar du droit d'accès, la carence légale d'un droit à l'information des personnes morales est compensée par l'existence d'obligations conventionnelles générales et spécifiques d'information. Également, des propositions de clauses relatives au droit d'information seront réalisées dans la section ci-après.

***271. Le droit à la portabilité***. Le droit à la portabilité dont bénéficient les personnes physiques au titre du RGPD ne s'applique pas davantage aux personnes morales. À l'instar des droits étudiés ci-dessus, cette carence légale est compensée dans le contrat cloud par l'intégration de la clause de réversibilité des données. La clause de réversibilité des données permet de garantir au client la possibilité de reprendre le contrôle exclusif de ses données et de ses applications. À titre

[579] Warusfel B. (sous la direction de Vivant M.), Le Lamy droit du numérique 2018, Expert, Partie 3 - Numérique et contrats, division 3 - Les principaux contrats du numérique et leurs spécificités, chapitre 6 - Les contrats d'informatique dématérialisée (cloud computing, p.490 n°704, mis à jour 22 avril 2022.

[580] Ibid.

[581] Conditions générales de service d'OVH (version du 6 mai 2022).

[582] Ibid.

illustratif, il est repris ci-après une clause de réversibilité : « en cas de cessation des relations contractuelles pour quelque cause que ce soit, le Prestataire s'engage à assurer une totale réversibilité des données appartenant au client, sur le plan technique et tout mettre en œuvre, sur les plans juridique et humain, afin de permettre au client de reprendre ou de faire reprendre par un tiers désigné par elle, l'administration des données du client. À ce titre, le Prestataire s'engage à fournir au Client, à sa demande, la copie sur « cartouche magnétique » de la dernière situation des données du client. En cas d'expiration ou de résiliation du contrat entre les parties, pour quelque motif que ce soit, le Client sera en droit d'obtenir du Prestataire que ce dernier lui communique toutes les informations qui lui seront nécessaires pour lui permettre de préparer la réversibilité des données (..) »[583]. En outre, le contrat cloud de la société PLANILOG précise concernant la réversibilité qu'en « cas de cessation des relations contractuelles pour quelque cause que ce soit, PLANILOG s'engage à restituer les Données au Client. Le Client pourra le cas échéant bénéficier d'une assistance de PLANILOG à la réversibilité sur devis. Sauf accord contraire des parties, la période de réversibilité est limitée à 30 jours »[584]. Par l'activation de cette clause, le client, personne morale, est en mesure de récupérer ses données à la fin du contrat. L'intégration de cette clause dans le contrat de cloud computing permet d'aboutir à une protection analogue à celle réservée aux personnes physiques pour l'exercice du droit à la portabilité. Dans ce sens, l'ingénierie contractuelle lorsqu'elle est efficacement employée permet de compenser, comme ici, les lacunes légales et aboutir au résultat escompté en matière de récupération des données.

***272.*** Après avoir observé que les personnes morales ne bénéficient pas d'un droit fondamental à la protection des données, il est étudié, à présent, si celles-ci peuvent prétendre à un droit à la vie privée comme fondement juridique à la protection de leurs données.

[583] Exemple de clause de réversibilité des données : Warusfel B. (sous la direction de Vivant M.), Le Lamy droit du numérique 2018, Expert, Partie 3 - Numérique et contrats, division 3 - Les principaux contrats du numérique et leurs spécificités, chapitre 6 - Les contrats d'informatique dématérialisée (cloud computing), p.494 n°712, mis à jour 22 avril 2022.

[584] Contrat cloud de Planilog concernant la mise en œuvre et de fourniture du service Planilog (Saas).

## B) L'absence d'un droit fondamental à la vie privée

***273.*** **Plan.** Dans le cadre de cette étude, il est observé que les juges refusent de reconnaître, au profit de la personne morale, un droit fondamental à la vie privée (1), mais ont admis certains droits issus du droit fondamental à la vie privée (2).

### 1) Le refus par les juges de la reconnaissance d'un droit à la vie privée des personnes morales

***274.*** ***Les fondements du droit à la vie privée*** : Bien qu'elle figure dans de nombreux textes[585], il est difficile de saisir les frontières du droit à la vie privée[586] en raison de l'absence d'une définition légale de la vie privée[587]. Pour compenser cette carence de définition, certains auteurs définissent le droit à la vie privée comme étant « la sphère secrète de la vie où chacun aura le droit d'écarter les tiers »[588]. Le juge a précédé le législateur en se fondant sur l'article 1382 du Code civil. Par la suite, « l'application de cet article 9 a d'ailleurs donné une nouvelle impulsion à la jurisprudence, qui s'est livrée à une interprétation très dynamique de ses dispositions »[589]. Le droit à la vie privée est, alors, l'œuvre d'une construction prétorienne façonnée complétée par l'article 9 du Code civil [590]. L'article 9 est rédigé en des termes généraux et que cette imprécision a permis au juge d'étendre son pouvoir d'interprétation. À cette interprétation dynamique du juge, il s'est posé la question de savoir si le juge n'est pas allé au-delà de son pouvoir d'interprétation en édifiant le régime du droit au respect de la vie privée. Concernant la délimitation de l'office du juge, Portalis avait indiqué, concernant la conception classique de la loi, que « le législateur fixe les principes, les règles générales, il ne descend pas dans les détails, il laisse ce soin au juge »[591]. En adhérant à cette conception classique de la loi, le risque est

[585] V. art. 8 de la CEDH.

[586] Martin L., le secret de la vie privée, RTD civ. 1959. 227, spéc. p. 230 : « Il paraît impossible, d'un mot, d'une formule, de dire à l'avance où finit la vie privée, où commence la vie publique. Il semble bien que cette question soit toujours dans la dépendance de l'appréciation souveraine des tribunaux ».

[587] Rapport Braibant, 3 mars 1998, Doc. fr., 1998.

[588] Carbonnier J., Droit civil des personnes, t.1,1996.

[589] Malaurie Ph., Les précédents et le droit, Revue internationale de droit comparé, 2006 58-2 pp. 319-326 : au sujet de l'art. 9 C. civ. : « La jurisprudence avait suscité la loi, la loi a nourri la jurisprudence ».

[590] La loi n° 70-643 du 19 juillet 1970 a introduit le droit au respect de la vie privée à l'article 9 du code civil et v. « le droit au respect de la vie privée est une création prétorienne façonnée à partir des dispositions relatives à la responsabilité pour faute des articles 1382 et suivants – désormais articles 1240 et suivants du code civil. La loi du 17 juillet 1970 a dans un second temps consacré et complété cette construction en modifiant l'article 9 du code civil qui énonce que « chacun a droit au respect de sa vie privée » : A. Basdevant et JP. Mignard, l'empire des données - essai sur la société, les algorithmes et la loi, Don Quichotte éditions, mars 2018, p.173.

[591] Conception classique de la loi par Portalis lors du discours préliminaire du code civil.

d'aboutir à ce que la jurisprudence soit « fluctuante, parfois casuistique, le cas échéant difficile à interpréter » laquelle s'illustre dans l'établissement du régime du droit à la vie privée[592].

***275.*** Le droit au respect de la vie privée dispose également d'un fondement constitutionnel tel que rappelé dans la décision du Conseil Constitutionnel[593]; il s'agit de l'article 2 de la Déclaration des droits de l'homme et du citoyen (DDH)[594] qui dispose que « le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme et que ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression, implique le respect de la vie privée ». Au niveau du droit international, l'article 12 de la Déclaration universelle des droits de l'homme[595] dispose que « nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance ni d'atteinte à son honneur ou à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ». Au niveau du droit européen, la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales[596], énonce à son article 8, paragraphe 1er, que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ». Il en découle que « l'apparition progressive des droits de la personnalité s'est faite sous l'action conjuguée de la loi et de la jurisprudence »[597]. En raison de son inscription dans différentes sources de textes, le droit à la vie privée profite d'une protection légale étendue. Cette réflexion des droits de la personnalité des personnes morales intéresse la matière du cloud puisqu'en cas d'admission de droits de la personnalité, la personne morale bénéficiera d'une protection renforcée de ses données.

***276. La transposition du droit à la vie privée au profit de la personne morale***. Le droit fondamental à la vie privée est conçu, initialement, au profit de la personne physique ; puis, la question du bénéfice de ce droit au profit de la personne morale s'est très vite posée. Autrement dit, est-ce que le fondement juridique du droit à la vie privée est transposable au profit de la personne morale pour permettre la protection de ses données ? Pour répondre à cette question, il

---

[592] Lepage A., Droits de la personnalité (Civ.), septembre 2009, dalloz.

[593] Décision du Conseil constitutionnel du 23 juillet 1999 : « « La liberté proclamée par l'article 2 de la DDH qui dispose que le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme et que ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression, implique le respect de la vie privée » : DC n° 99-416 du 23 juill. 1999 relative à la loi portant création d'une couverture maladie universelle, D. 2000. Somm. 265, obs. Marino L., CCE 1999. Comm. 52, obs. Desgorces R., RTD civ. 1999. 724, obs. Molfessis N. ; solution reprise dans la décision « loi relative au Pacs », nº 99-419 DC, 9 nov. 1999.

[594] La Déclaration des droits de l'homme et du citoyen (DDH) adoptée le 26 août 1789 et dont le Conseil constitutionnel a reconnu sa valeur constitutionnelle dans la DC n° 71-44 du 16 juillet 1971, constitutionnalité de la loi complétant les dispositions des articles 5 et 7 de la loi du 1er juillet 1901 relative au contrat d'association et la DC n° 73-51 du 27 décembre 1973, relative à la loi de finances pour 1974 ; il en résulte que la DDH est une norme de référence du contrôle de constitutionnalité exercé par le Conseil constitutionnel et dans la décision n°81-132 DC du 16 janvier 1982, ces droits et principes ont « pleine valeur constitutionnelle ».

[595] Déclaration universelle des droits de l'homme adoptée par l'Assemblée générale des Nations unies le 10 décembre 1948.

[596] Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, adoptée par la Conseil de l'Europe le 4 novembre 1950 et ratifiée par la France en 1974 (JO 4 mai).

[597] Lepage A., Droits de la personnalité (Civ.), septembre 2009, dalloz.

est proposé, ici, d'étudier les positions jurisprudentielles concernant l'extension des droits de la personnalité[598] aux personnes morales. En effet, il apparaît que le régime de la protection des droits de la personnalité des personnes morales est l'œuvre d'une construction prétorienne,[599] laquelle est appréhendée ci-après.

***277. L'absence d'un droit à la vie privée des personnes morales.*** Au niveau européen, la CJUE a, ainsi, décidé d'exclure explicitement et sans réserve les personnes morales du bénéfice du droit à la protection des données à caractère personnel associé au droit au respect de la vie privée[600]. La CJUE a retranscrit dans sa décision la dichotomie existante dans les textes européens et en particulier la directive « vie privée et communication électronique »[601] qui distingue « les droits et les libertés fondamentaux des personnes physiques et les intérêts légitimes des personnes morales, notamment eu égard à la capacité accrue de stockage et de traitement automatisé de données relatives aux abonnés et aux utilisateurs ». Les juges français refusent, également, d'admettre au profit de la personne morale un droit à la vie privée identique à celui des personnes physiques, et ce en se fondant sur l'article 9 du code civil[602]. Il s'agit d'une solution de principe qui a été confirmée dans un autre arrêt de 2018[603]. Ce refus par les juges empêche d'étendre la protection des données consacrée par la loi informatique et libertés au profit des personnes morales.

***278.*** Pour légitimer le refus d'un droit à la vie privée des personnes morales, les juges ont rappelé le principe de la distinction lequel est fonction des enjeux avec d'un côté, vie privée et liberté individuelle pour les personnes physiques et de l'autre secret des affaires pour les personnes morales[604]. Concernant cette dichotomie « vie privée et liberté individuelle pour les personnes physiques et de l'autre secret des affaires », certains auteurs ont considéré que cette exclusion n'aurait pas d'incidence concernant l'effectivité de la protection des données de la personne

---

[598] Théorie du droit défendue par Boistel selon laquelle il existe « des droits que l'homme apporte avec lui en naissant », lesquels préfigurent les droits de la personnalité, *Boistel* Philosophie du droit, 1889, t. I, nos 131 et s.

[599] Campagne N., Réalité et limites de la protection de la vie privée des entreprises, Revue Lamy Droit de l'Immatériel, Nº 101, 1er février 2014).

[600] CJUE, Gde ch., 9 nov. 2010, affaire n° C-92/09 et C-93/09, Volker und Markus Schecke.

[601] La Directive ePrivacy 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques ») modifiée par la suite par la directive 2009/136/CE du 25 novembre 2009. Elle vise à protéger les données et la confidentialité des communications en ligne. Cette Directive est en cours de révision et va laisser place à un Règlement. Ce nouveau projet de règlement ePrivacy est considéré comme étant « le « RGPD » des moyens de communication actuels et futurs ». Il vise à compléter les règles générales de protection des données à caractère personnel définies dans le RGPD concernant les données de communications électroniques. A la différence du RGPD, ce nouveau règlement étend la protection des données aux personnes morales. Ce règlement a, donc, vocation à s'appliquer à la protection des données des personnes physiques et des personnes morales.

[602] Civ. 1re, 17 mars 2016, pouvoir n°15-14.072, P I, n° 67 ; D. 2016. 1116, note G. Loiseau : Décision de la Cour de cassation, concernant l'absence d'un droit à la vie privée au profit des personnes morales au sens de l'article 9 du code civil.

[603] Civ. 1re, 16 mai 2018, pouvoir n° 17-11.210, non publié au bulletin.

[604] Pailler L., Pas de droit fondamental à la protection des données pour les personnes morales, Revue Lamy Droit de l'Immatériel, Nº 177, 1er janvier 2021.

morale puisque « le secret des affaires » est une notion très large qui permet d'intégrer dans son champ la protection demandée au titre de certains droits composant le droit au respect de la vie privée[605]. Dans ce sens, l'absence d'un droit à la vie privée au profit des personnes morales est compensée par l'établissement et l'application d'un régime légal spécifique qui est, le secret des affaires. Il est fait le choix, ici, de ne pas approfondir la notion du secret des affaires puisqu'elle sera étudiée plus amplement dans le cadre de la deuxième partie dédiée au renforcement de la protection des données des personnes morales[606].

**2) L'admission jurisprudentielle de certaines déclinaisons du droit fondamental à la vie privée**

***279.*** Le refus par les juges d'admettre un droit à la vie privée des personnes morales est constant et s'inscrit dans le prolongement des décisions qui ont étendu au profit de la personne morale certains droits composant le droit à la vie privée. L'admission de certaines déclinaisons du droit fondamental à la vie privée au profit de la personne morale est l'œuvre d'une construction prétorienne. Concernant la reconnaissance de certains droits composants le droit à la vie privée au profit des personnes morales, le Professeur P. Kayser a souligné qu'il ne peut s'agir de considérer « que la personne morale jouit à l'instar des personnes physiques d'un droit à la vie privée, entendu comme une vie intérieure, distincte de leur vie extérieure »,[607] mais plutôt de constater que la jurisprudence a reconnu certains droits composants le droit à la vie privée au profit de la personne morale similaire à ceux des personnes physiques[608]. Il en est ainsi de certains droits composant le droit à la vie privée, qui, dans le contexte du numérique, est défini comme la « capacité d'un individu à contrôler la collecte et l'utilisation de ses informations personnelles »[609]. Pour conforter, en France, la thèse de l'absence d'un droit à la vie privée des personnes morales, il a été jugé que « (…) si les personnes morales disposent, notamment, d'un droit à la protection de leur nom, de leur domicile, de leurs correspondances et de leur réputation, seules les personnes physiques peuvent se prévaloir d'une atteinte à la vie privée au sens de l'article 9 du Code civil »[610]. Cette décision permet de rappeler le principe selon lequel

[605] Gavalda C., Le secret des affaires, Mélanges René Savatier, Dalloz, 1965, p. 291.

[606] V. *infra* n° 622 et suivants.

[607] Kayser P., la protection de la vie privée par le droit, protection du secret de la vie privée, Economica, Presses Universitaires D'Aix-Marseilles.

[608] Campagne N., Réalité et limites de la protection de la vie privée des entreprises, Revue Lamy Droit de l'Immatériel, Nº 101, 1er février 2014.

[609] Warren S. et Brandeis L., The right to privacy, Harvard Law Review, 1890, vol. 4, nº 5, p. 193-220.

[610] Civ. 1re, 17 mars 2016, pouvoir n°15-14.072, P I, n° 67 ; D. 2016. 1116, note G. Loiseau : Décision de la Cour de cassation, concernant l'absence d'un droit à la vie privée au profit des personnes morales au sens de l'article 9 du code civil.

si la personne morale n'est pas titulaire d'un droit à la vie privée, elle dispose en revanche de certains droits dits de la personnalité qui sont attachés à la qualité de sujet de droit[611].

***280.*** En conséquence, par analogie aux droits des personnes physiques, les juridictions ont reconnu certains droits composant le droit à la vie privée au profit des personnes morales et en particulier la protection de leur domicile[612], de leur nom[613], de la réputation [614] ainsi que le droit au secret de la correspondance[615] et un droit à l'honneur[616] . Au niveau européen, la CEDH a, également, reconnu aux personnes morales sur le fondement de l'article 8 de la Convention européenne des droits de l'homme, la protection de l'activité et du domicile professionnels et a considéré que l'activité professionnelle n'était pas exclue de la protection de la vie privée au sens de l'article 8 de la Convention européenne des droits de l'homme[617]. La personne morale, sujet de droit, bénéficie, alors, de certains droits composant le droit à la vie privée.

***281.*** Il découle de cette construction prétorienne que la reconnaissance de certains droits de la personnalité au profit des personnes morales personnes morales permet à ces dernières d'hériter par accessoire, des actions et des procédures destinées à assurer la protection de ces droits[618]. La reconnaissance jurisprudentielle de ces droits au profit de la personne morale contribuerait, ainsi, à renforcer la protection des données dans les contrats de cloud computing. La personne morale, partie au contrat cloud, est en mesure d'invoquer certains droits issus du droit à la vie privée pour assurer la défense de ses droits en cas d'atteinte à ses données[619]. En revanche, le renforcement de la protection des données dans les contrats de cloud computing par l'admission de certains droits issus du droit fondamental à la vie privée est limité puisque ces illustrations jurisprudentielles ne concernent que certains droits composant le droit à la vie privée et non stricto sensu le droit à la vie privée.

***282.*** Il en résulte qu'en raison de l'absence d'une personnalité rattachée à l'humain, dans le sens de dignité de la personne humaine défendue à l'article 16 du Code civil[620], elle ne peut prétendre

---

[611] Carbonnier J., Droit civil, Les personnes, Thémis ; PUF, 20e éd. 1996, n° 225. – G. Cornu, Droit civil, Les personnes, Domat droit privé, Montchrestien, 13e éd. 2007, n° 99.

[612] Cass. ch. crim., 23 mai 1995, pourvoi nº 94-81.141, Bull. crim., nº 193, p. 524. V. également, CEDH 16 avr. 2002, Sté Colas Est c/ France, n° 37971/97.

[613] Cass. 1re civ., 8 nov. 1988, n° 86-13.264, JCP 1989. II. 21301, note R. Brichet, RTD com. 1989. 92 ; également v. Cass. 1re civ., 17 mars 2016, nº 15-14.072, RJDA 2016, nº 439, D. 2016, p. 2365.

[614] Cass. 1re civ., 17 mars 2016, pourvoi nº 15-14.072, RJDA 2016, nº 439, D. 2016, p. 2365.

[615] CEDH, 28 juin 2007, affaire 62540/00, Association for European Intégration and Human Rights and Ekimdzhiev c/ Bulgarie.

[616] Crim. 12 oct. 1976, pourvoi n° 75-90.239, Bull. crim. n°287, décision prise en application de l'article 32 de la loi du 29 juillet 1881.

[617] CEDH, 16 déc. 1992, affaire 13710/88, Niemietz c/ Allemagne, § 29, précité ; CEDH, 16 févr. 2000, aff. 27798/95, Amann c/ Suisse, § 65 ; et CEDH, 4 mai 2000, aff. 14566/05, Rotaru c/ Roumanie, § 43.

[618] Dumoulin L., Les droits de la personnalité des personnes morales, Revue des sociétés Dalloz, 2006.

[619] V. *supra* n° 279.

[620] L'article 16 du Code civil énonce que « la loi assure la primauté de la personne, interdit toute atteinte à la dignité de celle-ci et garantit le respect de l'être humain dès le commencement de sa vie ».

au bénéfice d'une protection légale par l'application du droit fondamental à la vie privée. Elle ne pourra, donc, pas agir sur le fondement juridique du droit à la vie privée pour protéger ses données faisant l'objet d'un contrat de cloud computing ; en revanche, elle pourra agir sur le fondement du droit au secret des affaires et les droits qui sont l'extension du principe du droit à la vie privée tel que le droit au domicile, à l'honneur et au secret des correspondances.

***283.*** Après avoir abordé l'inapplication des droits fondamentaux au profit de la personne morale, il s'agit d'étudier, à présent, les effets de l'absence d'un régime spécifique à la protection des données des personnes morales.

## Section 2 : Les effets de l'absence d'un régime spécifique à la protection des données des personnes morales

***284.*** Bien que soumises aux impératifs du RGPD lorsqu'elles collectent ou traitent des données à caractère personnel, les personnes morales ne bénéficient pas d'une réglementation équivalente et spécifique à la protection de leurs données et en particulier elles ne disposent pas du droit fondamental à la protection des données ainsi que le droit à la vie privée. Elles doivent donc veiller elles-mêmes à la protection de leurs données à caractère économique, stratégique et financier lors de la conclusion du contrat de cloud computing.

***285.*** **Plan.** Dans la plupart des cas, le prestataire de services cloud impose à son client, personne morale, un contrat cloud « standard » avec une marge quasi inexistante de négociation. Les effets de l'absence d'une réglementation spécifique à la protection des données des personnes morales apparaissent dans le cadre de la relation contractuelle (A) et dans le contenu du contrat de cloud computing (B).

### A) Dans le cadre de la relation contractuelle : l'abus de dépendance économique

***286.*** L'abus de dépendance économique au sein d'un contrat de cloud computing est appréhendé à travers l'étude des clauses. En particulier, la clause relative à la réversibilité des données revêt une importance fondamentale pour le client, dans le contrat de cloud computing, puisqu'elle lui garantit son indépendance vis-à-vis de son prestataire de services cloud (1). En pratique, il peut arriver que certains prestataires de services profitent de la dépendance économique de leurs clients en éludant dans le contrat la réversibilité des données (2).

**1) L'importance de la clause relative à la réversibilité des données**

***287.*** Les clauses relatives à la réversibilité et la transférabilité vers un autre prestataire sont requises afin de limiter le risque d'atteinte aux données stratégiques de l'entreprise. En effet, il y a un risque majeur et évident qu'un seul prestataire de services cloud, très souvent non-ressortissant du pays du client, puisse traiter l'ensemble des données de l'entreprise et parmi ces données figurent les données stratégiques lesquelles ont une valeur supérieure aux services fournis par le prestataire[621]. Cette inquiétude est d'autant plus légitime « lorsqu'un seul prestataire peut traiter toutes les données de toutes les plus grandes entreprises d'un ou plusieurs États étrangers à celui dont est ressortissant l'entreprise »[622].

***288.*** Les contrats de cloud computing sont régis « par un principe de récupération, des données par le client à la fin du contrat, mais cette évidence doit faire l'objet d'une clause précise. Il est recommandé de prévoir dans le contrat une clause de réversibilité qui permet au client de reprendre ou de faire reprendre son informatique externalisée par un autre prestataire, afin d'assurer la continuité de l'activité sans dégradation de la qualité »[623]. Il est important de prévoir dans le contrat ce qui se passe à la fin du contrat concernant les données et en particulier les conditions dans lesquelles le client pourra récupérer les données stockées. Très souvent, la réversibilité se résume à la restitution des données du client en leur dernier état de sauvegarde, laquelle est remise sur un support exploitable pour le client.

***289.*** Dans le cadre d'un contrat de cloud computing standard, il est plus adéquat de parler de « restitution des données » que de « réversibilité » des données. Cet engagement de restitution du prestataire de services cloud peut être traduit en termes contractuels de la manière suivante : au terme du contrat, le prestataire de services s'engage à remettre au « client une copie de l'ensemble des données en format standard, dans leur dernier état de conservation à la date de la demande, et détruit toute copie sur le serveur après information du Client »[624]. Lorsque le contrat de cloud computing offre au client des services personnalisés, comme l'intégration de logiciels tiers additionnels, la réversibilité réapparaît. La réversibilité inclut, en plus de la restitution des données dans un support standard exploitable, une prestation d'assistance pour la réalisation de

[621] Gaudrat Ph. et Sardain F., Traité de droit civil du numérique, Tome 2 Droit des obligations, édition Larcier 2015, p. 293, paragraphe 571.

[622] Ibid.

[623] Warusfel B. (sous la direction de Vivant M.), Le Lamy droit du numérique 2018, Expert, Partie 3 - Numérique et contrats, division 3 - Les principaux contrats du numérique et leurs spécificités, chapitre 6 - Les contrats d'informatique dématérialisée (cloud computing, p.494 n°712, mis à jour 22 avril 2022.

[624] Guide, Contractualisation de services cloud, les enjeux juridiques, Staub & Associes : https://www.eurocloud.fr/doc/guide-contractuel-cloud.pdf.

la migration des données et la reprise de logiciels. La clause déterminera, également, les tâches incombant à chacune des parties au contrat dans le cadre d'un plan de réversibilité.

***290.*** En raison de son importance, la clause de réversibilité nécessite d'être clairement définie et encadrée dans le contrat. Il est envisagé, ici, de ne pas approfondir la clause de réversibilité, puisqu'elle sera étudiée en seconde partie.

***291.*** À défaut de prévoir dans le contrat de cloud une clause de réversibilité permettant au client de reprendre ou de faire reprendre son informatique externalisée, le prestataire peut se voir reprocher un abus de dépendance économique.

**2) L'abus de dépendance économique en l'absence d'une clause de réversibilité des données**

***292.*** La notion d'abus de dépendance économique a été introduite en droit français par la loi du 30 décembre 1985,[625] qui « tient compte de la situation de dépendance économique du partenaire auprès duquel étaient pratiqués, demandés ou obtenus « des prix ou des conditions de vente discriminatoires ou encore des dons en marchandises ou en espèces dans des conditions de nature à porter atteinte à la concurrence", en tant que facteur aggravant justifiant que les peines applicables soient renforcées »[626].

***293.*** La dépendance était alors définie comme « une situation dans laquelle se trouve un partenaire commercial ne disposant pas de « solution alternative s'il souhaite refuser de contracter dans les conditions que lui impose son client ou son fournisseur »[627]. L'ordonnance du 1er décembre 1986[628] a, par la suite, consacré cette notion pour la réprimer en tant que « pratique anticoncurrentielle, au même titre que l'abus de position dominante, lorsqu'elle donne lieu à une exploitation abusive par un opérateur économique qui, même s'il ne domine pas un marché, domine un partenaire commercial dans un rapport bilatéral »[629].

---

[625] Loi du 30 décembre 1985, modifiant l'article 37 de l'ordonnance du 30 juin 1945 relative aux pratiques assimilées à la pratique de prix illicite (Ord. no 45-1483, 30 juin 1945, art. 37 1°, g mod. par L. no 85-1408, 30 déc. 1985). V. Pal. 1989, 1, chr., p. 290 ; Robin C., L'exploitation abusive d'un état de dépendance économique, LPA 28 juill. au 2 août 1989 ; Pirovano A. et Salah M., L'abus de dépendance économique : une notion subversive ? LPA 24 sept.1989.

[626] Chagny M. (sous la direction de), Le Lamy droit économique – Expert, 30 novembre 2020, Partie 2 Droit de la concurrence, Livre 3 Le contrôle des pratiques anticoncurrentielles, Titre 1 Le droit des pratiques anticoncurrentielles, Chapitre 6 Les pratiques anticoncurrentielles spécifiques au droit interne, Section 1 Les abus de dépendance économique, Sous-section 1 La prise en compte de la dépendance économique par la réglementation § 1. L'introduction de la notion dans le droit français, mis à jour 15/11/2021.

[627] Rapp. Colon, JO doc. Sénat 1985-1986, no 56, p. 24 ; Pedamon M., Les abus de domination, Cah. dr. entr. 1987/1, p. 15 ; Mousseron J.-M. et Sélinsky V., Le droit français nouveau de la concurrence, Litec, 1987, no 123 ; Mousseron J.-M. et Sélinsky V., Montagne ou souris : commentaire de la loi du 30 décembre 1985 portant amélioration de la concurrence, JCP E 1986, II, no 14682.

[628] Ord. no 86-1243, 1er déc. 1986, art. 8.

[629] Decocq A. et Pédamon M., L'ordonnance du 1er décembre 1986 relative à la liberté des prix et de la concurrence, J.-Cl. Conc. consom., no spéc. 1987, no 28 ; Thréard J. et Bourgeon Ch., Dépendance économique et droit de la concurrence, réflexions sur l'article 8 de l'ordonnance du 1er décembre 1986, Cah. dr. entr. 1987, Fasc. 2, p. 20 ; Sélinsky V., Abus de domination, J.-Cl. Cons.

***294.*** Dans le cadre d'un contrat de cloud computing, les conditions dans lesquelles les données seront, en pratique, stockées et transmises sont aussi importantes que la nature des prestations. En pratique, le sort des données à la fin du contrat peut revêtir plusieurs hypothèses. Soit, le prestataire conserve les données du client à la fin du contrat afin de permettre à ce dernier de les récupérer, soit les données sont immédiatement effacées à la fin du contrat, soit le prestataire refuse de préserver les données au-delà de la fin du contrat sans préciser que celles-ci seront effacées[630]. À titre illustratif, il est reproduit une clause du contrat cloud d'OVH qui informe le client de récupérer ses données avant la suppression du service : « 10.2 Le Client est seul responsable de faire en sorte que les opérations nécessaires (telles que la sauvegarde, le transfert vers une solution tierce, les instantanés, etc.) à la conservation des Données à caractère personnel soient effectuées, notamment avant la résiliation ou l'expiration des Services, et avant de procéder à toute opération de suppression, de mise à jour ou de réinstallation des Services. 10.3 À cet égard, le Client est informé que la résiliation et l'expiration d'un Service pour quelque raison que ce soit (incluant, mais de façon non exclusive le non-renouvellement), ainsi que certaines opérations de mise à jour ou de réinstallation des Services, peuvent automatiquement entraîner la suppression irréversible de tout Contenu (y compris les informations, données, fichiers, systèmes, applications, sites internet et autres éléments) reproduit, stocké, hébergé ou autrement utilisé par le Client dans le cadre des Services, ce compris toute sauvegarde potentielle »[631]. Compte tenu de cette rédaction, il incombe au client de récupérer ses données avant toute résiliation ou expiration du service. Cette clause concerne les données à caractère personnel et est contestable au regard du droit à la portabilité des personnes physiques. Si cette clause devait être intégrée dans un contrat cloud entre professionnels, elle serait sujette à discussion au regard de la prohibition de l'abus de dépendance économique.

***295.*** À ce titre et pour éviter toute censure, la société OVH pourrait indiquer, d'une part, que cette clause n'a pas pour effet d'empêcher la restitution des données et d'autre part, qu'elle propose son assistance à tout moment sur demande du client. Malgré cette justification, il n'en demeure pas moins que le client, qui se retrouverait dans une situation ne lui permettant pas de récupérer ses données (clause de réversibilité) ou de transférer ses données vers un autre prestataire, est en

---

conc., Fasc. 315, 1992, no 82 ; Pasqui G., L'abus de dépendance économique, Rev. conc. consom. 1993, no 71 ; Targa A., La notion d'atteinte à la concurrence sur le marché en droit français, Rev. conc. consom. 1993, comm. 76 ; Borra P., La notion de dépendance économique en droit français, AFEC, Journée du 8 janvier 1993, p. 31 ; De Mello X., Dépendance économique ou position dominante ? AFEC, Journée du 8 janvier 1993, p. 37 ; Brault D., Politique et pratique du droit de la concurrence en France, LGDJ : Droit des affaires 2004, no 946.

[630] Warusfel B. (sous la direction de Vivant M.), Le Lamy droit du numérique 2018, Expert, Partie 3 - Numérique et contrats, division 3 - Les principaux contrats du numérique et leurs spécificités, chapitre 6 - Les contrats d'informatique dématérialisée (cloud computing, p.494 n°712, mis à jour 22 avril 2022.

[631] Clauses 10.2 et 10.3 de l'annexe traitement de données à caractère personnel ou « DPA » des conditions générales de service d'OVH (version du 27 septembre 2021).

mesure d'invoquer l'abus de dépendance économique. Pour éviter de commettre un abus de dépendance économique constitutif d'une pratique anticoncurrentielle prohibée par l'article L. 420-2 du Code de commerce, le prestataire de services cloud devra, donc, prévoir dans le contrat de cloud computing une clause relative à la réversibilité et la transférabilité (vers un autre prestataire) afin de permettre à son client d'avoir une solution alternative lorsque ce dernier souhaiterait résilier le contrat[632]. Afin que la réversibilité soit effective, le client devra veiller à ce que la clause de réversibilité puisse prévoir les conditions de l'opération d'externalisation, les obligations de coopération à la charge du prestataire de l'externalisation et l'identification des éléments transférés afin d'aboutir, comme les juges du fond l'ont considéré, à « la restauration du statu quo ante »[633].

***296.*** Après avoir étudié l'impact de l'absence d'une réglementation spécifique à la protection des données des personnes morales dans le cadre de la relation contractuelle au travers de l'abus de dépendance économique, il s'agit de l'appréhender au travers d'une analyse des dispositions du contrat de cloud computing et en particulier du déséquilibre contractuel.

## B) Dans le contenu du contrat de cloud computing : le déséquilibre contractuel

***297.*** L'impact de l'absence d'une réglementation spécifique à la protection des données des personnes morales est perceptible, également, dans le contenu du contrat de cloud computing. Il est question d'étudier les clauses du contrat de cloud computing qui sont susceptibles de porter atteinte à la protection des données des personnes morales.

***298.*** **Plan.** Dans cette partie, il est envisagé d'étudier le déséquilibre entre les droits et les obligations des parties au contrat (1) et spécifiquement le droit d'information et de mise en garde (2).

[632] Développement de la clause de réversibilité (vs droit d'accès) : v. *infra* n° 314 et suivants.

[633] CA Paris, 14e ch., 4 juill. 1997, Expertises 1997, p.315.

**1) Le déséquilibre entre les droits et les obligations des parties**

***299. L'existence d'un déséquilibre contractuel*** : En pratique, la contractualisation du cloud computing se traduit par la standardisation du modèle contractuel[634]. Celle-ci s'explique par la nature même du cloud (mutualisation de l'infrastructure), des acteurs en cause (ETI[635], PME[636]) et de la durée des contrats. Dans cette configuration, les clients ne sont pas en position de négocier le contrat alors même que les demandes seraient légitimes. Toutefois, il existe des situations où certaines de ces entreprises vont pouvoir négocier le contenu du contrat de cloud computing. Les clauses qui attirent notre attention sont notamment celles relatives à la responsabilité (en cas de faute du prestataire, disponibilité du service, récupération des données), à la confidentialité des données, à la sécurité, à l'intégrité des données, à la réversibilité des données, à la résiliation et au droit applicable.

***300.*** Très souvent, le fournisseur de services cloud répond à une demande de négociation de son client que l'offre de services cloud est standard et que celle-ci ne peut faire l'objet de modification. Or, il est tout à fait possible de prévoir des modifications par la voie des avenants ou l'intégration de conditions particulières[637]. En cas de refus par le prestataire de services cloud, il sera possible de prétendre à la qualification du contrat cloud en contrat d'adhésion[638]. Quel est l'enjeu de cette qualification ? Il s'agirait de la possibilité d'invoquer le déséquilibre significatif entre les droits et les obligations des parties. Le déséquilibre significatif est apprécié spécifiquement selon qu'il est fait application des règles de droit commun ou celles de droit spécial.

***301.*** En droit commun des contrats, le déséquilibre significatif est prévu à l'article 1171 du code civil[639]. Cet article prévoit les critères d'admission du déséquilibre significatif. Tout d'abord, il faut qu'il s'agisse d'un contrat d'adhésion[640], être en présence d'une clause qui n'a pas été

---

[634] Le Tourneau Ph., contrats du numérique, informatiques et électroniques, Dalloz, 12e édition, 2022-2023, page 462 n°342.15 : « Pour une société importante, le contrat sera évidemment individualisé. Mais la majorité des contrats de cloud computing sont des contrats types ».

[635] ETI est un Sigle signifiant Entreprise à taille intermédiaire, il s'agit « d'une entreprise qui a entre 250 et 4 999 salariés, et soit un chiffre d'affaires n'excédant pas 1,5 milliard d'euros soit un total de bilan n'excédant pas 2 milliards d'euros », définition issue du site internet de l'INSEE, https://www.insee.fr/fr/metadonnees/definition/c2034.

[636] PME est un sigle signifiant Petite et moyenne entreprise, il s'agit « des entreprises qui, d'une part, occupent moins de 250 personnes, d'autre part, ont un chiffre d'affaires annuel n'excédant pas 50 millions d'euros ou un total de bilan n'excédant pas 43 millions d'euros », définition issue du site internet de l'INSEE, https://www.insee.fr/fr/metadonnees/definition/c1962.

[637] A ce titre, l'article 1119 du Code civil dispose qu'« en cas de discordance entre les conditions générales et les conditions particulières, les secondes l'emportent sur les premières ».

[638] Définition du contrat d'adhésion par l'article 1110 alinéa 2 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 ».

[639] 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. L'appréciation du déséquilibre significatif ne porte ni sur l'objet principal du contrat ni sur l'adéquation du prix à la prestation ».

[640] V. art. 1110 al. 2 C. civ.

négociée et laquelle créée un déséquilibre entre les droits et les obligations des parties. Ces critères sont cumulatifs. Ensuite, s'agissant de l'appréciation du déséquilibre significatif, il est précisé que celle-ci ne peut porter « ni sur l'objet principal du contrat ni sur l'adéquation du prix à la prestation »[641]. L'admission du déséquilibre significatif en droit commun des contrats permet de demander que la clause litigieuse soit considérée comme réputée non écrite[642]; ou encore d'invoquer une interprétation du contrat en faveur de la partie à qui est proposé le contrat[643]. La question se pose de savoir s'il est possible d'invoquer le déséquilibre significatif sur le fondement de l'article 1171 du code civil dans un contrat de cloud computing conclu entre des personnes morales agissant dans le cadre de leur activité professionnelle. La réponse à cette question nous est fournie par la Cour de cassation dans son arrêt en date du 26 janvier 2022[644] qui a jugé que l'article 1171 du Code civil s'applique aux contrats entre professionnels ne relevant pas du Code de commerce[645]. Pour rendre cette décision, la Cour de cassation s'est fondée sur les travaux parlementaires de la loi du 20 avril 2018 ratifiant l'ordonnance de 2016 et indique qu'il en ressort que « l'article 1171 du Code civil, qui régit le droit commun des contrats, sanctionne les clauses abusives dans les contrats ne relevant pas des dispositions spéciales des articles L. 442-6 du Code de commerce et L. 212-1 du Code de la consommation »[646]. Elle poursuit son raisonnement en considérant que « l'article 1171 du code civil, interprété à la lumière de ces travaux, s'applique donc aux contrats, même conclus entre producteurs, commerçants, industriels ou personnes immatriculées au répertoire des métiers, lorsqu'ils ne relèvent pas de l'article L. 442-6, I, 2° du code de commerce, dans sa rédaction antérieure à celle issue de l'ordonnance du 24 avril 2019 (..) »[647]. Depuis l'ordonnance du 24 avril 2019[648], l'article L. 442-6, I, 2º du Code de commerce est devenu l'article L. 442-1, I du code de commerce. Cet apport jurisprudentiel est louable puisqu'elle permet de clarifier le cadre de l'action fondée sur un déséquilibre significatif.

[641] V. art. 1171 C. civ.

[642] Ibid.

[643] Article 1190 du code civil « Dans le doute, le contrat de gré à gré s'interprète contre le créancier et en faveur du débiteur, et le contrat d'adhésion contre celui qui l'a proposé ».

[644] Cass. com., 26 janv. 2022, nº 20-16.782, B.

[645] De Roumeforts S., Déséquilibre significatif : premières précisions de la Cour de cassation depuis la réforme de 2016, Revue Lamy Droit civil, nº 201, 1er mars 2022.

[646] Cass. com., 26 janv. 2022, nº 20-16.782, B.

[647] Ibid.

[648] Ordonnance n° 2019-359 du 24 avril 2019 portant refonte du titre IV du livre IV du code de commerce relatif à la transparence, aux pratiques restrictives de concurrence et aux autres pratiques prohibées, JORF n°0097 du 25 avril 2019.

***302.*** En application de cette jurisprudence, lorsqu'il s'agit d'un contrat de cloud computing conclu par des personnes morales agissant en qualité de professionnels [649]qui relèvent de l'article L. 442-1, I du code de commerce (« toute personne exerçant des activités de production, de distribution ou de services ») [650], alors ce sont les règles spéciales du code de commerce qui s'appliquent et non celles de droit commun. En droit commercial, le déséquilibre significatif est 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 »[651]. À ce stade, la description du déséquilibre significatif est identique à celle du droit commun. En revanche, tous les contrats sont visés et non uniquement les contrats d'adhésion. Le déséquilibre significatif, ici, ne concerne pas seulement la conclusion et l'exécution du contrat, mais aussi la négociation commerciale[652]. Le champ d'application du déséquilibre significatif fondé sur l'article L. 442-1, I du code de commerce (ancien art. L. 442-6, I) est plus large que celui du droit commun des contrats de l'article 1171 du code civil. Par ailleurs, dans les contrats entre professionnels « il n'existe pas, à la différence du droit de la consommation, de mécanisme de catégorisation contraignant, comme peuvent l'être les listes de clauses réputées ou présumées abusives »[653]; également, « le texte n'exclut pas que le déséquilibre puisse résulter de la définition de l'objet principal du contrat ou de l'inadéquation du prix à la prestation »[654]. En droit commercial, le déséquilibre significatif est constitutif d'une pratique restrictive de concurrence qui a pour conséquence d'engager la responsabilité de son auteur et l'oblige à le réparer[655]. La sanction, en la matière, est l'engagement de la responsabilité de l'auteur de la pratique ; en l'espèce, il s'agirait du prestataire de services cloud. Il apparaît qu'à la suite de l'introduction du mécanisme par la loi de modernisation de l'économie du 4 août 2008, l'ordonnance n° 2019-359 du 24 avril 2019 a maintenu le principe d'une sanction du déséquilibre significatif, dont la

[649] Le professionnel est défini comme « toute personne physique ou morale, qu'elle soit publique ou privée, qui agit, y compris par l'intermédiaire d'une autre personne agissant en son nom ou pour son compte, aux fins qui entrent dans le cadre de son activité commerciale, industrielle, artisanale ou libérale » : Directive européenne n° 2011/83, art. 2, 2. Cette définition a été transposée en droit interne à l'article liminaire du code de la consommation par l'ordonnance no 2016-301 du 14 mars 2016, laquelle a ajouté l'activité agricole à la liste des activités professionnelles. V. Chantepie G., Sauphanor-Brouillaud N., Déséquilibre significatif, Répertoire de droit civil, Dalloz janvier 2022 (actualisation : Mars 2022).

[650] Article L. 442-1, I, 2° du code de commerce : « I. - Engage la responsabilité de son auteur et l'oblige à réparer le préjudice causé le fait, dans le cadre de la négociation commerciale, de la conclusion ou de l'exécution d'un contrat, par toute personne exerçant des activités de production, de distribution ou de services : (…)2° De soumettre ou de tenter de soumettre l'autre partie à des obligations créant un déséquilibre significatif dans les droits et obligations des parties ; (…) ».

[651] V. art. L. 442-1, I, 2° C. com.

[652] Ibid.

[653] Béhar-Touchais M., L'expansion stoppée de l'article L. 442-6, I, 2° du Code de commerce sur le déséquilibre significatif, RDC 2018. 67.

[654] Com. 25 janv. 2017, pourvoi nº 15-23.547, D. 2017. 481, note Buy F.

[655] V. art. L. 442-1, I, 2° C. com.

portée et les sanctions ont même été étendues[656]. La question s'était posée de savoir si au-delà de l'engagement de la responsabilité de l'auteur de la pratique, la victime (en l'espèce, le client, personne morale) peut demander l'inefficacité de la clause ? Sur ce point, la jurisprudence était fluctuante avant 2019. Certaines juridictions du fond ont rendu des décisions en faveur de l'admission de la nullité[657] et d'autres contre la nullité[658]. L'ancien article L. 442-6, I, du code de commerce, visait uniquement la responsabilité civile de l'auteur des pratiques[659]. Par ailleurs, la sanction de la nullité était réservée uniquement à l'action du ministre chargé de l'économie et le ministère public (ancien article L. 442-6, III du code de commerce[660]). L'ordonnance du 24 avril 2019 est venue consacrer l'action en nullité des clauses ou du contrat au profit de la victime[661] et l'a maintenue pour le ministre chargé de l'économie et le ministère public[662]. Dorénavant, l'article L. 442-4, I, alinéa 2 du code de commerce prévoit deux situations : toute personne justifiant d'un intérêt peut demander la cessation des pratiques mentionnées aux articles L. 442-1, L. 442-2, L. 442-3, L. 442-7 et L. 442-8 ; en revanche, seule la victime des pratiques peut faire constater la nullité des clauses ou contrats illicites et demander la restitution des avantages indus[663] (à l'exception du ministre chargé de l'économie et le ministère public[664]).

***303.*** Qu'en est-il de l'application de ce texte aux contrats informatiques et en particulier des contrats de cloud computing ? Il ne fait aucun doute, tel qu'affirme par la Professeure Béhar-Touchais, « que la forte concentration qui caractérise l'activité des géants de l'internet permet que les entreprises clientes soient « soumises » à un déséquilibre au sens de l'article L. 442-6, I, 2° du code de commerce »[665]. À cela, s'ajoute que « la notion de partenaire commercial, qui détermine le champ d'application de l'article L. 442-6, I, 2° du code de commerce, convient

---

[656] Behar-Touchais M., La réforme du titre IV du livre IV du code de commerce, JCP E 2019. 1361. – V. BUY F., La [décevante] réforme du droit des relations commerciales, D. 2019. 1122. – V. également, CHAGNY M., Quelle refonte du Titre IV du Livre IV du code de commerce après l'ordonnance n° 2019-359 du 24 avril 2019 ? JCP E 2019. 304.

[657] CA Paris, 29 oct. 2014, RG n°13/11059 ; CA Paris, 22 févr. 2017, RG n°16/17924.

[658] CA Versailles, 17 mars 2016, RG n°14/02990 ; CA Versailles, 31 mars 2016, RG n°14/02978 ; CA Paris, 18 mai 2016, RG n°14/12584 ; CA Paris, 6 sept. 2016, RG n°15/21026 ; CA Aix-en-Provence, 3 nov. 2016, RG n°14/13050 ; CA Toulouse, 7 déc. 2016, RG n°16/02774 ; CA Toulouse, 28 juin 2017, RG n°16/02093 ; CA Rennes, 4 juill. 2017, RG n°15/02244.

[659] Chantepie G., Sauphanor-Brouillaud N., Déséquilibre significatif, Répertoire de droit civil, Dalloz janvier 2022 (actualisation : Mars 2022).

[660] Version en vigueur du 11 décembre 2016 au 26 avril 2019 : les sanctions étaient les suivantes : ordonner la cessation des pratiques ; constater la nullité des clauses ou contrats illicites ; ordonner la répétition de l'indu ; ordonner la réparation des préjudices subis ; prononcer une amende civile ; ordonner « systématiquement » la publication, la diffusion, ou l'affichage de sa décision ou d'un extrait de celle-ci. Les juges du fond ont précisé que ces « sanctions peuvent être cumulées » : CA Paris, 21 juin 2017, RG n°15/18784.

[661] V. art. L 442-4 I, al. 2 C. com.

[662] V. art. L 442-4 I, al. 3 C. com.

[663] Chantepie G., Sauphanor-Brouillaud N., Déséquilibre significatif, Répertoire de droit civil, Dalloz janvier 2022 (actualisation : Mars 2022).

[664] V. art. L 442-4 I, al. 3 C. com.

[665] Béhar-Touchais M., L'expansion stoppée de l'article L. 442-6, I, 2° du Code de commerce sur le déséquilibre significatif, RDC 2018. 67.

parfaitement aux contrats conclus avec les géants de l'internet, et notamment des plateformes, dès lors qu'ils s'inscrivent dans la durée et sont destinés à développer l'activité des parties »[666]. Si ce texte est susceptible de s'appliquer aux contrats de cloud computing, encore faut-il pouvoir qualifier le déséquilibre contractuel. Autrement dit quelles sont les clauses pouvant être qualifiées de déséquilibrées. Pour identifier le déséquilibre du contrat, il est possible, tel que proposé par la Professeure Chantepie, de se fonder sur une appréciation théorique et une appréciation pratique[667]. Concernant l'appréciation théorique, le texte vise « un comportement », c'est-à-dire le fait de soumettre l'autre partie à des obligations créant un déséquilibre significatif[668]. Il en découle que l'identification du comportement doit « trouver son assise dans le contrat avant d'apprécier les critères du déséquilibre significatif »[669]. La prise en compte du comportement permet d'élargir la portée de ce texte ainsi que les sanctions[670]. Le comportement pourra, donc, être sanctionné lorsqu'il est de nature à créer un déséquilibre significatif entre les droits et obligations des parties. Le déséquilibre est apprécié selon un standard juridique reposant sur plusieurs critères et notamment la réciprocité ou la proportionnalité[671]. Le déséquilibre apparaît lorsqu'il existe une absence de réciprocité[672] ou de proportionnalité[673] à la condition que celle-ci atteigne un certain degré de gravité (en application de l'article L. 442-1, I, 2° (anc. art. L. 442-6, I, 2°), du code de commerce), c'est-à-dire que ce déséquilibre doit être « significatif »[674]. Par ailleurs, il a été précisé par la jurisprudence que l'appréciation du déséquilibre doit être réalisée « *in concreto* »[675], c'est-à-dire, dans « le contexte dans lequel il était conclu ou proposé à la négociation »[676], « au regard de l'économie de la relation contractuelle »[677]. Cette appréciation « *in concreto* »[678] a pour incidence que « celle des parties

[666] Ibid.

[667] Chantepie G., Sauphanor-Brouillaud, N., Déséquilibre significatif, Répertoire de droit civil, Dalloz janvier 2022 (actualisation : Mars 2022).

[668] T. com. Paris, 6 juill. 2021, n° 2016064825.

[669] Chantepie G., Sauphanor-Brouillaud, N., Déséquilibre significatif, Répertoire de droit civil, Dalloz janvier 2022 (actualisation : Mars 2022).

[670] CA Paris, 16 mai 2018, RG n° 17/11187.

[671] Fin-Langer L., L'équilibre contractuel, 2002, LGDJ, n^os^ 324 s.

[672] Elle est caractérisée, en général, par une absence de réciprocité des prérogatives contractuelles ou par une disproportion entre les droits et obligations des parties. Illustration : les juges du fond l'absence de « réciprocité et de contrepartie » de la clause : Com. 3 mars 2015, n° 15-27.525, AJCA 2015. 218, note Chantepie.

[673] Il s'agit d'une proportionnalité entre les droits et obligations des parties laquelle est analysée au travers d'une « analyse de l'équilibre contractuel » tenant compte tenant compte « de l'équilibre économique de l'opération ».

[674] CA Paris, 19 déc. 2018, RG n° 17/03922 : « une obligation financière dénuée de contrepartie pour celui à qui elle est imposée ne justifie aucune sanction lorsque, en raison de son faible coût, le déséquilibre qu'elle crée ne présente pas de caractère significatif ».

[675] CA Paris, 17 juin 2020, RG n° 18/23452, inédit.

[676] Com. 3 mars 2015, n° 14-10.907, inédit.

[677] CA Paris, 16 mai 2018, RG n° 17/11187.

[678] Com. 29 sept. 2015, n° 13-25.043 : les juges apprécient le déséquilibre significatif à partir d'une « appréciation concrète et globale des contrats en cause ».

qui en a imposé l'insertion dans le contrat peut encore montrer qu'elle était « nécessaire à l'équilibre de la convention ou que ce déséquilibre est compensé par d'autres dispositions du contrat »[679]. Concernant cette approche jurisprudentielle, la doctrine considère que « cette méthode est d'autant plus pertinente dans l'application de l'article L. 442-1, I, 2° (anc. art. L. 442-6, I, 2°), du code de commerce qu'il ne limite pas l'appréciation du déséquilibre significatif aux seules clauses abusives, mais permet la prise en compte d'un défaut d'équivalence des prestations »[680]. Tel qu'affirmé par certains auteurs, « le droit des pratiques restrictives de concurrence semble plus prometteur, notamment lorsqu'il permet de sanctionner le déséquilibre significatif »[681].

***304.*** Pour apprécier le déséquilibre contractuel au regard de la nécessité de préserver l'économie générale du contrat, il est envisagé d'étudier les clauses concernées. Tout d'abord, les clauses qui reconnaissent une prérogative à une seule des parties ou qui mettent un devoir à la charge d'une seule des parties, alors que la prérogative ou le devoir pourrait être réciproque[682]. Il s'agit, par exemple, des clauses de révision de prix en faveur uniquement de la partie qui a intégré cette clause[683], la clause résolutoire unilatérale dans certains cas[684], les clauses limitatives de responsabilité.

***305.*** Concernant la clause limitative de responsabilité, Microsoft l'a intégrée dans son contrat cloud dont le contenu peut prêter à discussion. Cette clause est prévue à l'article 7 du contrat cloud et stipule que « la responsabilité totale maximum de chaque partie envers l'autre, pour chaque produit, au titre du présent Contrat est limitée à des dommages et intérêts directs accordés en vertu d'une décision de justice définitive, dont le montant ne saurait excéder les montants dont le Client était tenu de s'acquitter pendant la durée du présent Contrat pour les produits concernés, sous réserve des conditions suivantes (..) c. Exclusions. Aucune des parties ne pourra être tenue responsable en cas de perte de revenus ou de dommage accessoire, spécial, incident, indirect, prononcé à titre de sanction ou exemplaire, ni en cas de perte de bénéfices ou de chiffre d'affaires, d'interruption d'activité ou de perte d'informations commerciales, quelle qu'en soit la cause et quel que soit le fondement de responsabilité invoqué »[685]. Il en découle

---

[679] Chantepie G., Sauphanor-Brouillaud N., Déséquilibre significatif, Répertoire de droit civil, Dalloz janvier 2022 (actualisation : Mars 2022).

[680] Ibid.

[681] Eréséo N., Libre circulation des données et droit de la concurrence (à propos du règlement du 14 novembre 2018 relatif à la libre circulation des données non personnelles), Dalloz IP/IT 2020 p.414.

[682] La lettre des réseaux, Déséquilibre significatif – Article 442-6, I, 2° du code de commerce, Panorama de jurisprudence 2016 - 2017 (116 décisions et avis commentés) : https://www.lettredesreseaux.com/P-2305-451-A1-desequilibre-significatif-article-442-6,-i,-2-du-code-de-commerce.html.

[683] CA Paris, 4 juill. 2013, RG n°12/07651 et CA Paris, 11 sept. 2013, RG n°11/17941.

[684] CA Paris, 30 mai 2017, RG n°16/24129.

[685] Contrat Microsoft Cloud, MCA2017Agr (NA)(FRE)(Sep20172).

que par l'intégration de cette clause dans le contrat, Microsoft a, d'une part, limité sa responsabilité en la plafonnant au montant payé par le client pour le produit concerné, et d'autre part, a éludé sa responsabilité en cas de pertes de données. Si cette clause peut apparaître contestable dans une certaine mesure à raison des limitations qu'elle fixe ; elle semble légale et non déséquilibrée, au regard de l'article L. 442-4, I du code de commerce, puisque la prérogative (ou le devoir) est réciproque entre les parties.

***306.*** Il existe, également, des clauses qui reconnaissent une prérogative exorbitante à l'une des parties ou mettent un devoir exorbitant à la charge d'une partie sans justification[686]. Sur ce point, les juges du fond ont eu l'occasion de statuer sur le déséquilibre allégué d'une clause limitative de responsabilité contenue dans un contrat de téléalarme laquelle stipulait que : « la responsabilité de la société ne saurait être engagée pour des dommages résultant du fonctionnement de l'installation ou de son non-fonctionnement pour quelque cause que ce soit, par exemple, le vol en l'absence d'une faute dûment prouvée par le client dans l'exécution des prestations prévues dans le présent contrat ». Les juges ont considéré que cette clause crée un déséquilibre significatif, « en ce qu'elle vide (…) le contrat de ce qui en fait l'essence même, à savoir le bon fonctionnement de la prestation d'alarme pour prévenir le vol »[687].

***307.*** Également, les clauses qui dérogent de manière répétée à des règles supplétives en faveur d'une partie[688] seront susceptibles d'être sanctionnées dès lors qu'elles créent un déséquilibre significatif. À titre illustratif, les juges du fonds ont sanctionné un ensemble de clauses qui faisaient supporter sur le fournisseur les risques que devait supporter le distributeur en sa qualité d'acheteur-revendeur[689] ; il s'agissait d'une clause de protection de stock[690], une clause de mévente des produits[691]. En l'espèce, il est reproché non pas le fait d'aménager le transfert des risques conventionnellement, mais de faire « supporter automatiquement l'intégralité de la charge du risque commercial (diminution de prix, mévente) sur le fournisseur » alors même qu'il a été constaté, par les juges du fond, « qu'à la suite du contrat de vente de son produit au profit de Darty, le fournisseur ne maîtrise plus le devenir de celui-ci sur le marché ».

---

[686] La lettre des réseaux, Déséquilibre significatif – Article 442-6, I, 2° du code de commerce, Panorama de jurisprudence 2016 - 2017 (116 décisions et avis commentés) : https://www.lettredesreseaux.com/P-2305-451-A1-desequilibre-significatif-article-442-6,-i,-2-du-code-de-commerce.html.

[687] CA Paris, 25 oct. 2016, RG n°14/20906.

[688] La lettre des réseaux, Déséquilibre significatif – Article 442-6, I, 2° du code de commerce, Panorama de jurisprudence 2016 - 2017 (116 décisions et avis commentés) : https://www.lettredesreseaux.com/P-2305-451-A1-desequilibre-significatif-article-442-6,-i,-2-du-code-de-commerce.html.

[689] CA Paris, 25 nov. 2015, RG n°12/14513 (affaire DARTY).

[690] Cette clause prévoyait qu'en cas de baisse de prix d'un produit, il était prévu au profit de DARTY un avoir correspondant à l'écart entre le précédent prix et le nouveau prix, multiplié par le nombre de produits en stock.

[691] Cette clause stipulait qu'en cas d'obsolescence d'un produit, d'arrêt de fabrication ou de mévente d'un produit, était prévu au profit de DARTY un avoir correspondant à l'écart entre le prix auquel le produit a été acheté par le client et le prix conforme à la situation nouvelle du marché à l'achat, multiplié par le nombre de produits en stock chez le client.

***308.*** Ensuite, il existe des clauses qui accordent des réductions de prix sans contrepartie à l'une des parties au contrat[692]. Concernant ces clauses, la Cour de cassation s'est prononcée sur la question des réductions de prix consenties par un fournisseur à un revendeur[693]. Elle a jugé que dans les rapports entre fournisseur et distributeur donnant lieu à la conclusion d'une convention récapitulative (en application de l'article L. 441-7 C. com.), les clauses de prix sans libre négociation des parties créent un déséquilibre significatif et constituent une pratique restrictive de concurrence.

***309.*** Le déséquilibre significatif étudié concerne la matière commerciale ; en revanche, lorsqu'il existe un déséquilibre significatif dans un contrat de cloud computing conclu entre une prestataire de services cloud et un consommateur[694] (personne physique qui n'agit pas en qualité de professionnel), alors ce sont les règles spéciales du code de la consommation qui s'appliquent et non celles du droit commun et ni celles du droit commercial. En particulier, c'est l'article L. 212-1 du code de la consommation[695] modifié par l'ordonnance du 14 mars 2016[696] qui a vocation à s'appliquer. Il est choisi de ne pas approfondir la question du déséquilibre significatif en droit de la consommation puisque celle-ci a fait l'objet d'une étude approfondie dans la partie qui concerne les personnes physiques[697].

***310.*** Après avoir envisagé les déséquilibres contractuels, il convient de poursuivre d'étude des lacunes légales à travers le contenu du contrat cloud et en particulier les clauses relatives au droit d'information, de mise en garde et du droit d'accès.

---

[692] La lettre des réseaux, Déséquilibre significatif – Article 442-6, I, 2° du code de commerce, Panorama de jurisprudence 2016 - 2017 (116 décisions et avis commentés) : https://www.lettredesreseaux.com/P-2305-451-A1-desequilibre-significatif-article-442-6,-i,-2-du-code-de-commerce.html.

[693] Cass. com., 25 janvier 2017, pourvoi n°15-23547, pub. Bull., confirmant CA Paris, 1 juill. 2015, RG n°13/19251 : La Cour de cassation a considéré que le déséquilibre significatif dans les droits et obligations des parties, dans les rapports entre un fournisseur et un distributeur, s'apprécie au regard de la convention écrite prévue par l'article L. 441-7 du code de commerce et « il suit de là que l'article L. 442-6, I, 2° du code de commerce autorise un contrôle judiciaire du prix, dès lors que celui-ci ne résulte pas d'une libre négociation et caractérise un déséquilibre significatif dans les droits et obligations des parties ».

[694] Article liminaire du code de la consommateur : le consommateur est défini comme étant « toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale ».

[695] V. article L.212-1 du code de la consommation : détermination des clauses abusives dans les contrats conclus entre professionnels et consommateurs.

[696] Ordonnance n° 2016-301 du 14 mars 2016 relative à la partie législative du code de la consommation, JORF n°0064 du 16 mars 2016.

[697] V. *supra* n° 158 et suivants.

**2) L'étude du droit d'information, de mise en garde et du droit d'accès**

***311. Le droit d'information et de mise en garde.*** Outre l'obligation générale de bonne foi prévue à l'article 1104 du Code civil[698] et l'obligation générale d'information précontractuelle prévue à l'article 1112-1 du Code civil[699] applicable à tous les contrats et mise en œuvre par les juges[700] ; il n'existe pas à l'heure actuelle une réglementation spécifique à la protection des données des personnes morales dans le cloud computing consacrant une obligation d'information spéciale à la charge du prestataire de services de cloud computing. Le droit à l'information des données des personnes morales n'est pas prévu par la loi et, donc, constitue à ce jour une lacune légale pour la protection des données de ces personnes.

***312.*** Il en résulte que le prestataire de services n'est pas obligé d'insérer dans le contrat de cloud une disposition relative au droit d'information de la personne morale. Il apparaît, en pratique, que les contrats de cloud computing standard ne prévoient pas une obligation de conseil, d'information et de mise en garde à la charge du prestataire de services cloud. Il incombe, donc, au client de veiller à ce que cette lacune légale soit compensée par l'insertion, dans le contrat de cloud computing, d'une disposition relative au droit d'information accompagnée d'une obligation de mise en garde du prestataire de services cloud (notamment en cas de transfert de données hors de l'Union européenne).

***313.*** À titre illustratif, il est repris ci-après un modèle de clause de mise en garde du contrat cloud de la société Planilog : « Préalablement à la conclusion du contrat, le client est informé qu'il doit s'entourer de tous les conseils nécessaires à s'assurer que les modules répondent à ses besoins et à l'usage qu'il en attend. Planilog n'assume aucune responsabilité du fait d'une erreur de choix, d'appréciation du Client ou de l'inadéquation des modules à ses besoins »[701]. Cette clause, qui a pour objet d'avertir le client quant à la pertinence par ce dernier des choix de services cloud, pourra être alimentée en fonction des besoins des parties et de l'opération cloud concernée.

En outre, il apparaît opportun d'annexer à cette clause de mise en garde, une clause relative au droit d'information du client, laquelle devrait contenir à notre sens les informations relatives au traitement des données (identification des données susceptibles d'être traitées), le lieu de

[698] Principe générale de bonne foi dans les contrats : Article 1104 du code civil : « Les contrats doivent être négociés, formés et exécutés de bonne foi. Cette disposition est d'ordre public ».

[699] Principe de l'obligation générale d'information dans les contrats : v. art. 1112-1 du code civil.

[700] Les juges ont été amenés à statuer sur la question du droit à l'information du client et de l'obligation de mise en garde du prestataire de service et ont estimé que « le prestataire de service à l'obligation d'informer son client, et même de le conseiller, en lui communiquant toute donnée qui pourrait lui être utile » : Warusfel B. (sous la direction de Vivant M.), Le Lamy droit du numérique 2018, Expert, Partie 3 - Numérique et contrats, division 3 - Les principaux contrats du numérique et leurs spécificités, chapitre 6 - Les contrats d'informatique dématérialisée (cloud computing, p.490 n°704, mis à jour 22 avril 2022.

[701] Extrait du contrat de mise en œuvre et de fourniture du service Planilog (SaaS), Article 6 mise en garde, V14032017, p.2.

stockage (hébergement) des données et de la localisation des serveurs. Un modèle de clause relative à la communication des informations de localisation et de sécurisation des données est proposé en deuxième partie dédiée au renforcement de la protection des données par l'ingénierie contractuelle[702].

***314.*** Il en résulte que l'absence d'un droit à l'information peut être compensée par l'insertion de clauses relatives à un devoir d'information du prestataire envers le client. À l'instar du droit à l'information, il n'existe pas à l'heure actuelle d'un droit d'accès aux données au profit des personnes morales.

***315. Le droit « d'accès » aux données versus la disponibilité des données dans le cloud.*** En matière de cloud computing, il ne s'agit pas d'appliquer « le droit d'accès » tel que consacré pour la protection des données à caractère personnel[703] qui permet « de savoir si des données (..) sont traitées et d'en obtenir la communication dans un format compréhensible (..), de contrôler l'exactitude des données et, au besoin, de les faire rectifier ou effacer »[704], ni de garantir « l'accès » aux données puisque le client par principe dispose de la maîtrise de ses données en y accédant directement dans le cloud. Il s'agirait plutôt à travers cette notion de « droit d'accès » d'imposer au prestataire une obligation de disponibilité des données, c'est-à-dire de pouvoir garantir au client que les données ainsi stockées soient présentes dans le cloud et disponibles sans interruption au profit du client lorsqu'il accède au cloud. À l'instar du droit à l'information, il en résulte que le prestataire de services n'est pas obligé de prévoir dans le contrat de cloud une disposition relative au droit d'accès des données des personnes morales. En revanche, il apparaît que si le prestataire de services de cloud computing n'assure pas la disponibilité des données dans le cloud, un tel manquement pourrait être constitutif d'une inexécution contractuelle ouvrant droit à réparation au profit du client. En effet, la garantie « d'accès » (disponibilité) aux données au profit des personnes morales figure comme étant une des obligations principales du contrat de cloud computing. Le prestataire de services cloud intègre, très souvent, malgré l'absence d'une obligation légale spécifique relative au droit « d'accès », des dispositions relatives à la disponibilité des données, et ce au travers des clauses « de réplication des données » [705] et « de réversibilité des données »[706].

---

[702] V. *infra* n° 660 et suivants.

[703] Art. 15 du RGPD : « La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel (..) ».

[704] https://www.cnil.fr/fr/le-droit-dacces-connaitre-les-donnees-quun-organisme-detient-sur-vous.

[705] Définition : La clause de réplication des données envisage de dupliquer « les données sur d'autres sites distants et feront ensuite l'objet d'une restauration dans des délais et modalités prédéfinis » : Alix P. et Perfetti G., VIRTUALEGIS cabinet d'avocats, Les contrats de cloud computing : les clauses importantes du point de vue des clients, 24 novembre 2012 (https://www.legavox.fr/blog/virtualegis/contrats-cloud-computing-clauses-importantes-10101.htm)

***316.*** Il est repris, ci-après, une clause permettant d'informer le client des conditions de l'accès aux données : « l'accès aux Données est réservé au seul Client. Toutefois, pour les seuls besoins liés aux services, le prestataire pourra également y accéder. Cet accès aux Données par le prestataire ne pourra être que temporaire. Ce dernier devra veiller à ne pas endommager les Données et à ne plus permettre aucun accès à celles-ci dès que les raisons ayant justifié son intervention auront cessé. Le prestataire s'engage à prendre toutes les mesures de sécurité conformes à l'état de l'art concernant le contrôle d'accès logique, et au minimum sans que cette liste soit limitative, celles prévues à l'Annexe « Sécurité » du présent Contrat. Le prestataire s'engage notamment à conserver la trace horodatée des actions réalisées dans son système d'information (notamment flux émis et reçus, nouvelles versions applicatives, tests, erreurs, les dé-doublonnages et les purges etc.) à des fins de contrôle, d'audit et de preuves. Conformément à l'Annexe « Sécurité », le prestataire tient à la disposition du client un journal d'événements sécurisés contenant les traces de connexion aux Données et des opérations effectuées par les utilisateurs finaux et le prestataire et, le cas échéant, par toute autre personne, et ce pendant une durée d'un (1) an à compter de l'enregistrement de chacune de ces traces. Le client est informé et accepte que le prestataire puisse accéder à ses Données et les transmettre sur réquisition d'une autorité administrative ou judiciaire habilitée à accéder aux Données. Sauf si ladite réquisition l'en empêche, le prestataire veillera à informer le client sans délai de l'existence de la réquisition et des données qui ont été transmises. »[707].

***317.*** Si une telle clause permet, en effet, d'informer expressément le client des conditions d'accès aux données, il apparaît que les droits ainsi conférés par cette clause sont sujets à discussion et devraient faire l'objet d'une analyse *a priori* du client avant la conclusion du contrat. Il s'agirait d'étudier, en amont de la signature du contrat cloud, les droits du client et du prestataire que confère cette clause d'accès aux données et d'envisager les répercussions de ces droits sur la protection des données des personnes morales. Par exemple, le fait de conférer un droit d'accès au prestataire non justifié et non limité par des considérations objectives, techniques et réelles pourrait menacer la protection des données, en particulier sa sécurité et son intégrité. Il est fondamental que les parties au contrat puissent définir le cadre du droit d'accès aux données (de la disponibilité) dans le contrat de manière équilibrée afin de préserver la sécurité et l'intégrité des données des personnes morales.

---

[706] V. *infra* n° 717 et suivants.

[707] Martin N. et Auvieux C., article 9.2, extrait du formulaire ProActa, Lamyline, FII.345-5 Contrat de fourniture de solutions et de prestations informatiques en mode SaaS.

***318.*** En définitive, il apparaît que l'existence des lacunes légales concernant la protection des données des personnes morales dans le cloud computing est réelle en raison de l'absence d'un droit d'information, de mise en garde ou d'un droit d'accès, mais celles-ci vont pouvoir être compensées par l'ingénierie contractuelle.

# Conclusion du chapitre 1

***319. L'existence d'un vide juridique en matière de protection des données des personnes morales dans le cloud computing.*** À l'instar des données à caractère personnel, il n'existe pas de réglementation spécifique à la protection des données des personnes morales dans le cloud computing. Dans le cadre d'un contrat cloud entre un client, personne morale, et un prestataire de services cloud, le règlement général à la protection des données n'a pas vocation à s'appliquer aux données afférentes à la personne morale. Également, elles ne bénéficient pas de droits fondamentaux à la protection de leurs données et à la vie privée. L'absence d'une réglementation spécifique à la protection des données des personnes morales est perceptible dans le cadre de la relation contractuelle avec la constatation de déséquilibres contractuels et d'abus de dépendance économique. En raison de ces lacunes légales, les personnes morales doivent veiller elles-mêmes à la protection de leurs données à travers une analyse des dispositions du contrat de cloud computing et une ingénierie contractuelle.

# Chapitre 2 : L'absence d'un régime spécifique au transfert des données des personnes morales

***320. La perte de contrôle des données***. Dans le cadre d'un contrat de cloud computing, les données sont confiées à un tiers (le prestataire) auquel il faut faire confiance. On perçoit, alors, les risques pour ces clients de laisser leurs données transiter hors de leurs propres installations. L'utilisation de la technologie du cloud computing par la personne morale l'oblige, alors, « à se déposséder de la maîtrise technique de son système d'information et d'accepter que ses données soient stockées chez le prestataire »[708]. À ce jour, les principales inquiétudes des personnes morales quant à l'utilisation d'un cloud sont liées notamment à la sécurité, la confidentialité, l'intégrité des données et à la qualité de service.

***321. La nécessité d'un cadre légal***. Concernant le droit applicable à la protection des données des personnes morales, il a été observé dans les développements précédents que le RGPD ne s'applique pas aux données des personnes morales puisqu'elles ne sont pas considérées comme étant des données à caractère personnel[709]. Les données des personnes morales sont considérées comme étant des données à caractère non personnel[710]. En matière de transfert des données au sein de l'Union européenne, c'est le règlement européen (RDNP) du 14 novembre 2018[711] qui s'applique. L'objectif de ce texte est d'assurer le libre flux des données non personnelles au sein de l'Union en établissant un corps de règles relatives aux exigences de la localisation des données[712]. Ce texte a, également, le mérite de poursuivre « une finalité bien plus limitée », qui est l'établissement d'un cadre adapté pour déployer l'informatique en nuage et promouvoir, ainsi, les services de cloud computing[713]. Ce texte est spécifique aux données à caractère non personnel, lesquelles englobent, donc, les données des personnes morales. En revanche, ce texte se limite à édicter une réglementation à la libre circulation des données au sein de l'Union européenne et n'a pas vocation à traiter du transfert de ces données hors de l'Union européenne.

---

[708] Mallet-Poujol N., Le Lamy droit du numérique, expert, sous la responsabilité de Vivant M., Partie 3 Numérique et contrats, Division 3 Les principaux contrats du numérique et leurs spécificités, Chapitre 6 Les contrats d'informatique dématérialisée (cloud computing), Section 2 Avantages et contraintes des prestations de cloud, Contraintes et risques des prestations de cloud, mis à jour 04/2022.

[709] V. *supra* n° 10 et v. RGPD, art. 4.

[710] V. *supra* n° 16 et v. RDNP, art.4.1.1.

[711] Règlement (UE) numéro 2018/1807 du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne dit RDNP :https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018R1807&from=El.

[712] Art. 1er du RDNP.

[713] Carre S., Libre circulation des données, propriété et droit à l'information : à propos du règlement (UE) 2018/1807 du 14 novembre 2018, Dalloz IP/IT 2020.

***322.*** **Plan.** Il est procédé à l'étude, tout d'abord, du cadre juridique de la circulation des données au sein de l'Union européenne (section 1) puis, du vide juridique en matière de transfert des données des personnes morales hors de l'Union européenne (section 2).

## Section 1 : L'application imparfaite du cadre légal de la circulation des données au sein de l'Union européenne

***323.*** Le transfert des données à caractère non personnel (incluant donc les données des personnes morales) au sein de l'Union européenne est encadré par règlement européen (RDNP) lequel a, donc, vocation à s'appliquer au contrat de cloud computing conclu entre un client, personne morale, et un prestataire de services.

***324.*** **Plan.** Il est proposé d'étudier le cadre légal européen applicable à la circulation des données à caractère non personnel au sein de l'Union européenne (A) suivi d'une analyse critique (B) afin d'en mesurer l'impact sur la protection des données des personnes morales dans les contrats de cloud computing.

### A) L'identification du cadre de la circulation des données au sein de l'Union européenne

***325.*** **Plan.** L'Union européenne a consacré les principes de libre circulation des données et de réduction des exigences de localisation des données (1) ainsi que le portage des données (2).

#### 1) La consécration des principes de libre circulation des données et de réduction des exigences de localisation des données

***326.*** ***La logique libérale de la circulation des données.*** Les services de cloud computing sont très souvent des services transnationaux et suscitent des questions juridiquement complexes. Dans un contexte de mondialisation et de libre-échange au sein de l'espace économique européen (EEE), la difficulté consiste à établir un équilibre entre « la protection des données » et « la liberté de commerce et d'industrie »[714]. Pour préserver cet équilibre, il apparaissait plus que

[714] Art. 7 de la loi des 2 et 17 mars 1791 dite « décret d'Allarde » instituant le principe de la liberté du commerce et de l'industrie puis confirmé par la loi des 14 et 17 juin 1791 dite « Le Chapelier ». V. Décision n° 81-132 DC, 16 janvier 1982, Loi de nationalisation, cons. 16.

nécessaire d'établir une réglementation soucieuse de la préservation de cet équilibre entre d'un côté « protection des données » et de l'autre « liberté de commerce et d'industrie ». Le RDNP s'inscrit, ainsi, dans le cadre de la construction d'un marché unique du numérique, défini comme « un espace dans lequel la libre circulation des biens, des personnes, des services et des capitaux est garantie (…) où les particuliers et les entreprises peuvent accéder et développer des activités en ligne, dans un cadre garantissant une concurrence loyale et un niveau élevé de protection des consommateurs et des données personnelles »[715]. Il s'agirait, ainsi, de surmonter les ambitions nationales au sein de l'Union européenne afin de parvenir à une volonté commune pour la création d'un marché unique de la donnée. À cette fin, l'Union européenne s'est dotée de mesures complémentaires telles que « la sanction des États récalcitrants, le standard de reconnaissance mutuelle (..), l'adoption d'objectifs communs, tels qu'assurer une compatibilité interne des mesures ou un haut niveau de protection de certaines personnes ou intérêts, ou encore la défense d'un modèle européen vis-à-vis des acteurs étrangers ». En raison de cette évolution, certains auteurs ont pu affirmer que « la liberté de circulation s'est peu à peu départie d'une simple logique de suppression des restrictions pour devenir une méthode d'organisation des conditions de la mobilité au sein du marché intérieur ». Cette ambition d'un marché unique de la donnée nécessite la libéralisation du marché européen de la donnée[716] en raison pour laquelle des principes vont être affirmés.

***327. L'affirmation du principe de libre circulation des données au sein de l'Union européenne.*** Le principe affirmé, par le RDNP, est la libre circulation des données à caractère non personnel dans l'Union européenne, qui sont qualifiées de « marchandises immatérielles »[717]. Les données non personnelles sont identifiées comme englobant « par défaut l'ensemble des données numériques qui n'entrent pas dans le champ des données personnelles telles que définies par le RGPD. Il peut s'agir, ainsi, de données commerciales, de données sur l'agriculture, de précision, sur les besoins d'entretien des machines, météorologiques, etc. »[718]. Les données des personnes morales sont considérées par défaut comme des données à caractère non personnel. Il est visé que cette marchandise immatérielle puisse « être transférée et gérée là où le souhaitent ses détenteurs auprès de fournisseurs-hébergeurs dans des pays autres que celui de sa création

[715] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279.

[716] Communiqué IP/18/4227 du 19 juin 2018, JCP E 2018.Actu. 528 : La Commission européenne précise que le RGPD et le règlement sur le libre flux des données à caractère non personnel fonctionneront ensemble pour permettre la libre circulation de toutes les données (à caractère personnel et non personnel) et créer ainsi un espace européen unique des données.

[717] Avis du Comité économique et social européen sur la « Communication de la Commission au Parlement européen et au Conseil — Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne », publié au Journal officiel de l'Union européenne, le 15 janvier 2020.

[718] V. *supra* n° 16.

ou de son utilisation au sein de l'Union européenne »[719]. Alors même que les personnes morales ont des inquiétudes sur la sécurité de leurs données hébergées dans le cloud computing, le RDNP acte le principe de la libre circulation des données à caractère non personnelles au sein de l'Union européenne.

***328.*** Le principe de la libre circulation des données à caractère non personnel au sein de l'Union européenne est affirmé à l'article 4 du RDNP, lequel interdit toute restriction quant à la localisation des données sauf si elles sont justifiées par des motifs de sécurité publique dans le respect du principe de proportionnalité[720]. Ce principe est composé du principe de la libre circulation et du principe de réduction des exigences de la localisation des données. Ce texte[721] ne concerne que les données à caractère non personnel et ne s'applique pas aux services de traitement des données ayant lieu en dehors de l'Union européenne ni aux exigences de localisation relatives à ces données[722]. En outre, il est identifié deux types d'obstacles à la libre circulation des données (« free flow of data »)[723]; il s'agit « des réglementations nationales en matière de localisation des données »[724] d'une part, et « les pratiques menant à une dépendance à l'égard des fournisseurs dans le secteur privé, d'autre part »[725]. À partir de ce constat, le texte impose de manière explicite[726], l'élimination de « toute forme de restriction géographique s'agissant du stockage des données »[727]. Ces restrictions peuvent prendre la forme de législations nationales imposant des exigences de localisation des données dans le pays concerné ainsi que des dispositions contractuelles ne permettant pas le client de changer facilement de fournisseur.

***329.*** Concernant la mise en œuvre de ce principe, « l'élimination des entraves s'est d'abord faite par des interdictions adressées aux États membres d'introduire ou de conserver des mesures qui généraient ou empêcheraient la libre circulation dans le domaine économique. Il s'agissait alors d'interdire d'interdire »[728]. Le RDNP a eu, donc, pour incidence de faire lever toutes les exigences relatives à la localisation des données[729]. Sur le fondement de l'article 4 du RDNP, il

---

[719] Art. 1er du RDNP.

[720] Art. 4 du RDNP.

[721] Art. 2 du RDNP.

[722] Considérant 15 du RDNP.

[723] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ?, RTD Eur. 2021 p.279.

[724] Considérant 4 du RDNP.

[725] Considérant 5 du RDNP.

[726] Mouchette J., Haro sur les obligations de localisation des données non personnelles, Dalloz IP/IT 2021 P.401).

[727] Zolynski C., La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne, Dalloz IP/IT 2020 p.429.

[728] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279.

[729] Art. 2 du RDNP.

est demandé aux États membres non seulement de ne pas adopter des dispositions ayant pour effet de restreindre la circulation des données à caractère non personnel, mais également de supprimer toutes celles qui sont en vigueur[730].

***330. Le principe de réduction des exigences de localisation des données***. Pour la construction d'un marché unique de la donnée, le RDNP exige des États membres « de réduire au minimum leurs exigences de localisation des données, ainsi que la fragmentation des législations en la matière de façon à stimuler la croissance et à libérer les capacités d'innovation des entreprises »[731]. Par cette disposition, ce sont les cloud souverains qui sont visés. L'enjeu de la libéralisation des données est la croissance de l'économie et le développement des innovations. Il est rappelé que « les données électroniques sont au centre de ces systèmes et peuvent générer une grande valeur lorsqu'elles sont analysées ou combinées à des services et des produits »[732]. Afin d'être compétitive au niveau international, l'Union européenne a, donc, décidé de se doter de ce texte favorable à la construction d'un marché unique des données au sein de l'Union européenne. Il s'agissait, ainsi, de « briser les barrières nationales en matière de réglementation des télécommunications, de droit d'auteur, de protection des données, en matière de gestion des ondes radio et d'application du droit de la concurrence »[733].

***331. La sécurité publique, l'exception à la libre circulation des données.*** La limite au principe de libre circulation des données à caractère non personnel au sein de l'Union, conformément à l'article du 4 du RNDP, est la sécurité publique[734]. Il en découle qu'il n'est pas permis, pour un État, d'exiger la localisation des données dans « un pays » sauf si la sécurité du pays concerné est menacée. Le concept de sécurité publique englobe la sécurité intérieure et extérieure d'un État membre ainsi que les questions de sûreté publique[735]. Cette limite n'est pas spécifique au principe de la libre circulation des données, mais correspond à une restriction commune à l'ensemble des libertés consacrées par le droit de l'Union européenne (liberté de circulation des capitaux, biens, services et personnes)[736]. À l'exception de cette limitation, le règlement n'en contient aucune autre.

---

[730] Ibid.

[731] Avis du Comité économique et social européen sur la « Communication de la Commission au Parlement européen et au Conseil — Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne », publié au Journal officiel de l'Union européenne, le 15 janvier 2020).

[732] Considérant 1 du RDNP.

[733] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279.

[734] Art. 2 du RDNP.

[735] Considérant 19 du RDNP.

[736] Mouchette J., Haro sur les obligations de localisation des données non personnelles, Dalloz IP/IT 2021 P.401.

***332. Une circulation sans conditions.*** Le scepticisme doctrinal[737] sur l'efficacité de cette réforme en ce qui concerne les stratégies européennes sur la « data », fait naître, en pratique, des interrogations sur le plan informatique[738], économique[739] et juridique[740]. En matière juridique, alors que pour les données à caractère personnel le principe de libre circulation des données est conditionné au respect des principes découlant du RGPD et doit, donc, être conforme aux principes « de licéité, loyauté et transparence ; limitation des finalités ; minimisation des données ; exactitude ; limitation de la conservation ; et intégrité et confidentialité »[741], les données à caractère non personnel circulent librement au sein de l'Union européenne et hors de l'Union européenne. Il s'agit, alors, de s'interroger sur le point d'équilibre entre la protection des données des personnes morales dans le cloud computing et la construction d'un marché unique des données au sein de l'Union européenne. L'application du RDNP au niveau européen a pour conséquence que les données des personnes morales peuvent être transférées librement au sein de l'Union européenne sans restriction et sans nécessité de recueillir au préalable le consentement de la personne morale. C'est dans ces conditions qu'il est possible d'affirmer que la personne morale perd en quelque sorte la maîtrise de ses données stockées dans le cloud computing alors même que « les données constituent désormais un élément essentiel de leur patrimoine informationnel »[742].

***333.*** De plus « au contraire d'une marchandise qui n'existe que dans un seul exemplaire tangible, l'objet numérique n'est en nombre limité que par une convention choisie ou imposée aux intermédiaires de la circulation »[743].

***334.*** Si le RDNP consacre un principe de libre circulation des données et de réduction des exigences de localisation des données, il permet également de conférer le portage des données au profit des personnes morales.

---

[737] Zolynski C., La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne, Dalloz IP/IT 2020 p.429.

[738] Grossa J., Les données non personnelles : un *tech checking*, Dalloz IP/IT 2020. 213.

[739] Guichardaz R. et Pénin J., L'économie de la réutilisation des données (non personnelles), Dalloz IP/IT 2020.

[740] Favro K., Les données non personnelles : un nouvel objet juridique, Dalloz IP/IT 2020. 234.

[741] Art. 5 du RGPD.

[742] Zolynski C., La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne, Dalloz IP/IT 2020 p.429.

[743] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279.

**2) La consécration du portage des données des personnes morales**

***335. Un « portage » fondé sur des mécanismes d'autorégulation.*** Afin d'assurer la libre circulation des données, la Commission européenne a rappelé que les données deviennent mobiles et peuvent donc faire l'objet de « portage ». Pour garantir la mobilité des données, le RDNP prévoit le portage des données au profit des personnes morales. Aucune restriction de localisation des données ne peut avoir lieu au sein de l'Union européenne. Pour renforcer l'effectivité du « portage », la Commission a encouragé les fournisseurs de services à mettre en œuvre des codes de conduite[744]. Ce texte autorise les acteurs à définir le cadre de leurs relations contractuelles et notamment l'exercice du portage et ce en encourageant l'élaboration de codes de conduite[745]. Le « portage » des données à caractère non personnel consacré par le RDNP fait écho au « droit à la portabilité » consacré par le RGPD au profit des personnes physiques. Malgré des points de convergence, ces droits conservent leurs singularités.

***336.*** Le droit à la portabilité, conformément à l'article 20 du RGPD, permet aux personnes physiques : « de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle (…) ». Quant au « portage » des données à caractère non personnel, l'article 6 du RDNP[746] indique que « la Commission encourage et facilite l'élaboration de codes de conduite par autorégulation au niveau de l'Union afin d'établir notamment les bonnes pratiques qui facilitent le changement de fournisseurs de services et le portage des données dans des formats structurés, usuels et lisibles par machine, notamment dans des formats standard ouverts, lorsque le fournisseur de services obtenant les données le demande ou l'exige ; (..)». Dans ces conditions, le RDNP « ne prévoit pas le droit pour les utilisateurs professionnels de transférer les données, mais a une approche autorégulatrice, avec des codes de conduite volontaires pour les entreprises »[747].

---

[744] Art. 6 paragraphe 3 du RDNP : « La Commission encourage les fournisseurs de services à terminer le développement des codes de conduite au plus tard le 29 novembre 2019 et à les mettre effectivement en œuvre au plus tard le 29 mai 2020 ».

[745] Zolynski C., La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne, Dalloz IP/IT 2020 p.429.

[746] Art. 6 du RDNP.

[747] Communication de la commission au parlement européen et au conseil, lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'union européenne, du 29 mai 2019, p.20 : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52019DC0250&from=FR. V. également article 6 du RDNP. V. également, Zolynski C., La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne, Dalloz IP/IT 2020 p.429.

***337.*** Il s'agit, alors, de s'interroger si le « portage » des données à caractère non personnel permet de contribuer au renforcement de la protection des données des personnes morales au sein de l'Union européenne. Il est possible de s'apercevoir que la teneur du droit à la portabilité et le portage n'est pas identique en matière de sécurité juridique. Alors que le RGPD confère un droit à la portabilité des données au profit des personnes physiques[748], le RDNP accorde aux personnes morales la possibilité d'organiser « le partage »[749] des données au travers de l'établissement de code de conduite[750]. Le droit à la portabilité est un droit fondé sur le RGPD, c'est-à-dire encadré par la régulation », alors que le portage est organisé selon les codes de conduite adoptés. Cette différence de nature fera l'objet d'une analyse critique approfondie dans le développement qui suit.

***338.*** Indépendamment de cette différence de nature, l'objectif est la construction d'un marché unique du numérique, laquelle passe nécessairement par l'harmonisation des règles au sein de l'Union européenne. L'uniformisation des règles applicables au sein de l'Union européenne est une exigence fondamentale afin de pouvoir garantir une sécurité juridique et éviter une distorsion de concurrence[751]. À ce titre, certains auteurs considèrent que ce cadre serait adapté pour déployer l'informatique en nuage et contribuerait à l'essor des services de cloud computing et plus particulièrement, la concurrence entre les services de cloud computing[752]. En revanche, pour d'autres auteurs, ce cadre européen ne serait pas effectif en raison de l'inadaptation des principes consacrés aux spécificités de la donnée numérique hébergée dans une infrastructure cloud.

***339.*** Ainsi, il apparaît que si des principes sont consacrés pour rendre effective la libre circulation des données au sein de l'Union européenne, des critiques peuvent être formulées.

[748] Art. 20 du RGPD.

[749] Art. 6 du RDNP.

[750] Ibid.

[751] Considérant 7 du RDNP.

[752] Zolynski C., La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne, Dalloz IP/IT 2020 p.429.

## B) Des principes inadaptés à la protection des données des personnes morales

***340.*** **Plan.** De cette analyse du cadre légal européen des données à caractère non personnel, des critiques peuvent être formulées au regard de la protection des données des personnes morales hébergées dans le cloud. Tout d'abord, il apparaît que le portage est fondé sur « un droit mou » (1), puis que les critères géographiques sont inappropriés en raison d'une part, de la capacité de duplication des données et d'autre part, du déficit d'infrastructure informationnelle européen (2).

### 1) Un portage des données fondé sur un « droit mou »

***341.*** La doctrine a critiqué le RDNP quant à la reconnaissance du « portage » des données au profit des personnes morales en considérant que « le texte ne reconnaît qu'un ersatz de droit à la portabilité par comparaison au modèle que constitue le RGPD s'agissant des données personnelles »[753]. Cette observation fait allusion à l'absence d'un droit contraignant concernant la mise en œuvre du « portage » au profit des personnes morales. En effet, cette préconisation du RDNP n'est en rien une obligation contraignante. Il s'agit, alors, d'une différence fondamentale entre les deux règlements puisque « l'un s'appuie sur le droit dur, l'autre sur des instruments non contraignants (soft Law) »[754] par le biais d'un mécanisme d'autorégulation que sont les codes de conduite dont l'article 6 du RDNP fait état[755].

***342.*** Selon certains auteurs, ce texte « ne fait qu'inciter les opérateurs à livrer à leurs cocontractants une information relative aux clauses de réversibilité stipulées au sein des contrats de services de cloud computing, sans imposer la reconnaissance d'un droit à la portabilité, ni même une obligation d'information relative à la réversibilité des données » puisqu' « aucune disposition contraignante ne figure à ce titre dans le règlement »[756]. Le mécanisme d'autorégulation promu par ce texte se confronte à un scepticisme de la doctrine concernant son efficacité. Pour certains auteurs, « l'autorégulation montre en effet trop souvent ses limites lorsque les rapports entre opérateurs laissent apparaître une forte asymétrie de pouvoir, ce qui caractérise pleinement les contrats liant les utilisateurs aux prestataires de cloud computing »[757].

---

[753] Bougeard A., Les dispositions relatives à l'accès et au portage des données : code de conduite et bonnes pratiques, Dalloz IP/IT 2020 p.408.

[754] Avis du Comité économique et social européen sur la « Communication de la Commission au Parlement européen et au Conseil — Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne », publié au Journal officiel de l'Union européenne, le 15 janvier 2020. V. également, Zolynski C., La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne, Dalloz IP/IT 2020 p.429.

[755] Art. 6 du RDNP.

[756] Zolynski C., La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne, Dalloz IP/IT 2020 p.429.

[757] Ibid.

Cette situation de déséquilibre de « pouvoir »[758] est constatée, par exemple, dans les contrats d'adhésion conclus entre des prestataires qui dominent le marché des prestations de services cloud et les clients, personnes morales.

***343.*** Par conséquent, si l'on opère un comparatif entre le droit à la portabilité accordé aux personnes physiques et le portage des données des personnes morales, la différence est majeure. Par ce constat, il est possible de considérer que cette différence de nature juridique entre « le droit à la portabilité et « le portage » constitue une lacune légale quant à la protection des données des personnes morales. Malgré ce constat, les personnes morales devraient pouvoir bénéficier, aujourd'hui, d'un portage dès lors que le prestataire de services cloud l'a prévu dans son code de conduite ou dans le contrat cloud. Par ailleurs, si le portage n'est pas un droit « contraignant », des sanctions sont susceptibles d'être prononcées dès lors que le fournisseur établit des restrictions à la mise en œuvre du « portage ». À ce titre, la jurisprudence a considéré « que tous les comportements et toutes les clauses ayant pour effet d'entraver le changement de fournisseur sont susceptibles de recevoir la qualification d'abus de position dominante »[759]. Dans ce sens, « le droit de la concurrence pourrait être considéré comme un instrument utile pour sanctionner les abus de position dominante »[760] des fournisseurs de services cloud « dominants ». À titre illustratif, en Allemagne, le Bundeskartellamt[761] dans sa décision du 7 février 2019 a considéré « qu'une violation du règlement (UE) 2018/1807 puisse constituer un abus d'exploitation pouvant être sanctionné au titre d'un abus de position dominante »[762] ; décision qui a été confirmée par la Cour fédérale allemande[763]. Il en découle que si le contrat de cloud computing contient des clauses faisant soit obstacle soit limitant l'exercice du portage créant ainsi des entraves au changement de fournisseur cloud, alors la qualification d'abus de position dominante est susceptible de s'appliquer.

***344.*** Outre, la critique d'un portage fondé sur « un droit mou », il est mis en lumière que les critères géographiques établis sont inappropriés au renforcement de la protection des données des personnes morales hébergées dans le cloud computing.

---

[758] Ibid.

[759] Eréséo N., Libre circulation des données et droit de la concurrence (à propos du règlement du 14 novembre 2018 relatif à la libre circulation des données non personnelles), Dalloz IP/IT 2020 p.414. V. CJUE 13 févr.1979, aff. C-85/76, Hoffmann-La Roche c/ Commission. V. TPICE 17 sept. 2007, aff. T-201/04, Microsoft Corp. c/ Commission des Communautés européennes, D. 2007. 2303, obs. Chevrier E..

[760] Eréséo N., Libre circulation des données et droit de la concurrence (à propos du règlement du 14 novembre 2018 relatif à la libre circulation des données non personnelles), Dalloz IP/IT 2020 p.414.

[761] Il s'agit d'une autorité allemande de la concurrence.

[762] Art. 6 du RDNP.

[763] Décision rendue par le Bundesgerichtshof, le 23 juin 2020, n° 080/2020.

**2) Des critères géographiques inappropriés**

***345.*** Les critères géographiques, ainsi, établis par l'Union européenne, semblent inappropriés à la protection des données des personnes morales hébergées dans le cloud au regard de la capacité de duplication des données numériques (a) et du déficit d'infrastructure informationnelle européen (b).

a) La difficile délimitation géographique en raison de la capacité de duplication des données

***346. La capacité de duplication des données dans le cloud***. Aujourd'hui, la logique empruntée par l'UE est fondée sur « les potentialités de réplication offertes par le numérique » et sur une approche libérale des données. L'Union européenne acte la libre circulation des données au sein de l'Union européenne et établit, ainsi, une cinquième liberté[764] de la circulation sur le marché unique européen. À cette fin, l'Union européenne supprime les frontières, les obstacles et les barrières au sein de l'Union européenne telles que les règles de localisation des données. L'approche entreprise par l'Union européenne a été critiquée par la doctrine qui estime que « cette approche purement libérale a rapidement rencontré ses limites, consistant, d'une part, dans la mauvaise volonté des acteurs, qui masquent leur inertie en « déguisant » les restrictions, d'autre part, dans l'absence de cohérence du résultat produit une fois les entraves retirées. Enfin, le caractère purement économique des libertés consacrées s'est peu à peu heurté au développement d'une ambition politique de plus grande envergure au sein de l'Union »[765]. L'Union européenne a construit ce principe dans une logique de représentation spatiale de l'objet. Si le règlement (UE) 2018/1807 a permis de consacrer une 5e liberté de circulation[766], ou du moins, tel qu'affirmé par certains auteurs, une « méta-liberté »[767] ; elle est critiquée par la doctrine en raison de sa vision, semble-t-il, « étriquée » de la libre circulation des données[768], « du flou de son champ d'application et du caractère essentiellement « ubiquiste » des objets numériques » [769]. Ils critiquent la volonté de la construction d'un marché unique des données par la consécration de la libre circulation comme une « 5e liberté », en estimant que « la liberté de circulation des activités numériques se loge difficilement dans les frontières géographiques de l'Union.

[764] Boev I., Le nouveau règlement : un 5e principe de libre circulation ? Dalloz IP/IT 2020. 223

[765] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279.

[766] Ibid.

[767] Ibid.

[768] Zolynski C., La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne, Dalloz IP/IT 2020 p.429.

[769] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279. V. également, Thèse de Berthillon F., L'ubiquité des biens, soutenue publiquement le 18 déc. 2020, à l'Université de Lyon 3.

***347.*** La consécration d'un principe de libre circulation des données dans un espace géographiquement déterminée (au sein de l'Union européenne) n'est pas adaptée puisque le flux des données est par principe mobile et se caractérise par sa capacité à se dupliquer instantanément sur des terminaux distincts situés à des endroits géographiquement dispersés des uns des autres. Par la capacité de duplication[770], les données peuvent se retrouver instantanément dans des infrastructures différentes situées hors des frontières de l'Union européenne. C'est en raison de la difficulté à localiser les données en un seul endroit à un seul moment que la circulation des données doit être envisagée autrement que dans « le monde analogique »[771]. C'est parce que « la donnée numérique » est un objet qui ne peut être circonscrit matériellement à un espace géographique figé dans le temps qu'il semble difficile de consacrer une liberté de circulation telle que promue par ce texte. C'est pourquoi certains auteurs considèrent que « la circulation dans le secteur numérique doit se démarquer des représentations attachées au monde analogue, en ouvrant la voie au partage »[772]. Il s'agirait de passer d'une logique de « circulation linéaire à une circulation de partage »[773]. Non seulement les infrastructures sur lesquelles reposent les échanges utilisent également la duplication des informations, la plupart du temps hors de l'Union, pour optimiser les flux, mais de surcroît, les plus gros acteurs économiques sont eux-mêmes localisés en dehors du territoire.

***348.*** Pour ces raisons, il paraît difficile d'envisager une liberté de circulation propre au marché « intérieur » européen, alors que la circulation numérique s'opère à une plus grande échelle »[774]. En effet, la spécificité des données numériques est une mobilité des données fondée sur « la reproduction éclatée dans l'espace »[775]. Il en résulte que la construction d'un marché unique des données avec la consolidation du principe de libre circulation des données au sein de l'Union européenne n'est pas adaptée pour assurer la protection des données des personnes morales dans le cloud computing. Ces critiques mettent en lumière les difficultés à surmonter pour protéger de manière effective les données des personnes morales dans les contrats de cloud computing.

---

[770] La circulation des données se caractérise par la duplication, explication : « La circulation repose, techniquement, sur un mécanisme de « reproduction ». Les informations transitent par des réseaux qui assurent leur communication par des processus de duplication. Si, dans le monde analogique, on note que X1 étant le premier lieu et X2 un second lieu, quand un élément (a), va de X1 à X2, soit X1(a)-a = X2(0) + a, alors n(a) est invariable, quel que soit X. La valeur transférée est stable. À l'inverse, dans le cadre d'un ensemble réticulaire s'apparentant à une toile d'araignée (le web, par exemple) ou à un rhizome, tel qu'un réseau numérique, le passage de (a) de X1 à X2 se notera X1(a) + X2(a), et ainsi de suite, soit n(a) = n(X). Il y a donc, potentiellement, autant « d'exemplaires » de l'élément circulant que de lieux de circulation. La valeur transférée est susceptible de croître par cet effet de multiplication » : Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279.

[771] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? p.279, *op. cit.*.

[772] Ibid.

[773] Ibid.

[774] Ibid.

[775] Ibid.

***349.*** Outre la capacité de duplication des données, il est envisagé d'établir la critique des critères géographiques au regard du déficit d'infrastructure informationnelle européen.

b) Un déficit d'infrastructure informationnelle européen

***350. La remise en cause des cloud souverains.*** Les dispositifs visés, par le principe de réduction des exigences de localisation des données, sont les « clouds souverains »[776]. La justification pour l'utilisation du cloud souverain est de protéger la personne morale contre la délocalisation de ses données hors des frontières de l'État et ainsi de réduire les risques d'atteinte à celles-ci. C'est ainsi, concernant les personnes morales de droit public, qu'une circulaire administrative a été adressée aux administrations pour donner instruction aux administrations décentralisées de recourir à un « cloud souverain »[777]. Dorénavant, la France et les autres États membres doivent se conformer à compter du 31 mai 2021 à l'esprit à la lettre de ce nouveau texte. En conséquence, il n'est plus permis pour un État membre de conserver ou d'adopter des dispositions faisant obstacle à la libre circulation des données à caractère non personnel au sein de l'Union européenne sauf à pouvoir justifier d'un intérêt de sécurité publique[778]. En dépit de cette interdiction, les opérateurs conservent la liberté de déterminer contractuellement la localisation des données,[779] mais cette liberté dans les contrats de cloud computing est très souvent « favorable aux fournisseurs de service de cloud »[780].

***351. Un déficit d'infrastructure informationnelle européen***. La nouvelle stratégie de la Commission met l'accent sur le nécessaire développement d'une souveraineté numérique européenne[781]. La Commission européenne invite au développement d'infrastructures locales qui permettraient de s'affranchir de la tutelle technologique d'opérateurs venant des États tiers. Depuis une dizaine d'années, plusieurs projets d'un « cloud européen » sont portés sans qu'aucun n'aboutisse effectivement[782]. Aujourd'hui, le projet d'un cloud européen, intitulé Gaia-

[776] V. *supra* n° 329.

[777] Note d'information du 5 avril 2016 relative à l'informatique en nuage (Cloud computing), Réf. NOR MCCC1614354C.

[778] V. *supra* n° 330.

[779] Boev I., Le nouveau règlement : un 5e principe de libre circulation ? Dalloz IP/IT 2020 ; V. également, Carre S., Libre circulation des données, propriété et droit à l'information : à propos du règlement (UE) 2018/1807 du 14 novembre 2018, Dalloz IP/IT 2020.

[780] Zolynski C., La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne, Dalloz IP/IT 2020 p.429.

[781] Quiviger P.-Y., Une approche philosophique du concept émergent de souveraineté numérique, NCCC 2017, n° 57, p. 25 ; Türk P., La souveraineté des États à l'épreuve d'internet, RD publ. 2013. 1489.

[782] Les projets cloud Andromède (2011-2012) et de CloudWatt (contrôle repris à 100 % par Orange en mars 2015) et Numergy (contrôle repris à 100 % par SFR en décembre 2015) se sont soldés par des échecs : Le Quellenec E., Huin L., Benchetrit A., Korabelnikov D., Cloud computing et droit, retour sur une année de grands changements**,** Revue Lamy Droit de l'Immatériel, N° 138, 1er juin 2017**.**

X[783], est « co-porté avec des opérateurs américains du Cloud »[784]. Ces derniers se sont engagés à garantir que « le traitement se déroulera exclusivement sur le territoire de l'Union »[785]. Les entreprises se sont engagées « à déclarer où et comment sont opérées les données qu'elles manipulent, à faciliter le passage d'un service de cloud à un autre, à permettre l'interopérabilité entre les services, et à garantir la souveraineté des données »[786]. Il s'agit uniquement d'un engagement de droit privé du prestataire de services qui trouve sa limite lorsqu'une autorité publique d'un état (et notamment, ici, les États-Unis) exige le transfert des données sur le fondement d'un acte ayant une portée extraterritoriale.

***352. La remise en cause de l'effectivité du cadre européen face à des opérateurs cloud étrangers.*** Dans cette configuration, il peut paraître utile de supprimer les entraves à l'intérieur de l'Union et de renforcer l'effort d'harmonisation pour limiter les différences de traitement, mais la finalité recherchée (la protection des données dans un marché unique de la donnée) pourrait échouer si les opérateurs en charge d'assurer les transmissions, le stockage, les traitements des flux sont étrangers et ne sont pas soumis aux règles européennes. Cette observation est illustrée, ici, avec le recours à une solution technique américaine, la Plateforme *Health Data Hub*, pour gérer des données de santé en France[787]. Il en résulte que « dans ces conditions, la consécration d'une cinquième liberté de circulation profitera, au premier chef, aux acteurs extraeuropéens déjà extrêmement puissants sur le marché européen[788]. Plus encore, si la proposition du règlement DMA[789] « cherche à corriger ces asymétries, c'est bien le développement industriel, et non le droit seul, qui peut apporter un remède efficace au déficit d'infrastructures informationnelles européennes »[790]. Dans ce sens, bâtir un marché unique de la donnée fondé uniquement sur l'établissement de règles serait insuffisant pour assurer la protection des données, il faudrait pouvoir donner naissance à des prestataires de services européens pouvant concurrencer les prestataires étrangers.

---

[783] Le Quellenec E., L'émergence d'un cloud souverain européen, Revue Lamy Droit de l'Immatériel, N° 173, 1er août 2020.

[784] Lancé en mars 2020, autour de vingt-deux entreprises françaises et allemandes, il associe, depuis nov. 2020, plus de 180 entreprises émanant de dix-huit États, dont douze États membres de l'Union. Outre *OVH* (français), se sont jointes les grandes figures (étrangères) du Cloud, telles *Amazon, Google, Microsoft, Alibaba*, et du logiciel, comme *Oracle, Salesforce* ou *Palantir*.

[785] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279. V. également, Thèse de Berthillon F., L'ubiquité des biens, soutenue publiquement le 18 déc. 2020, à l'Université de Lyon 3.

[786] Ibid.

[787] CE, ord. réf., 13 oct. 2020, n° 444937 ; Bertrand B., Polyphonie dans l'appréciation du recours à une solution technique américaine pour la Plateforme *Health Data Hub* : le Conseil d'État et l'art de la fugue, JCP n° 49, 30 nov. 2020, 1358.

[788] À titre illustratif, Google détient plus de parts de marché, en tant que moteur de recherche, en Europe qu'aux Etats-unis. En France en 2020, Google est en situation monopolistique, il vient en tête, avec 92,06 % des parts du marché, suivi de Bing avec 3,95 % des parts du marché et Yahoo avec 1,6 % des parts de marché, puis Ecosia, Qwant et DuckDuckGo, se partagent le reste des parts du marché avec chacun 1,23 %, 0,72 % et 0,32 % (source des statistiques : StatCounter).

[789] V. *supra* n° 24.

[790] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279.

***353.*** Après avoir étudié le cadre légal de la circulation des données des personnes morales au sein de l'Union européenne, il est envisagé d'analyser les principes applicables lors d'un transfert de données hors de l'Union européenne.

## Section 2 : L'absence de cadre légal pour le transfert des données des personnes morales hors de l'Union européenne

***354.*** **Plan.** Bien que le RDNP soit spécifique à la circulation des données à caractère non personnel, il ne régit pas le transfert des données hors de l'Union européenne. L'absence de règles pour transférer les données des personnes morales hors de l'Union européenne constitue une lacune légale (A). En revanche, cette lacune légale pourrait être compensée en cas d'adoption d'une nouvelle réglementation (B).

### A) L'existence d'un vide juridique

***355.*** Dans cette partie, l'existence d'un vide juridique est appréhendée par l'étude d'une part, des lacunes légales perceptibles dans le cadre de l'externalisation des services cloud à l'étranger (1), et d'autre part, des effets juridiques sur la loi du contrat et la compétence juridictionnelle (2).

#### 1) Une lacune légale dans le cadre de l'externalisation des services cloud à l'étranger

a) Une différence de protection injustifiée entre les données personnelles et les données des personnes morales

***356.*** ***Un besoin de protection des données des personnes morales.*** La sous-traitance « se prête tout particulièrement à l'externalisation du stockage des données et au cloud computing »[791] et engendre de facto une fragilisation « de la sécurité de la relation principale entre la personne concernée et le responsable de traitement : elle créé un risque s'agissant du respect du droit des données personnelles par le sous-traitant »[792]. Dans le cadre d'un contrat de cloud computing, le prestataire de services cloud (entrepreneur principal) dispose de la faculté de sous-traiter à un autre professionnel (le sous-traitant) une partie des obligations conventionnelles et notamment celles relatives à l'hébergement des données dans des serveurs. En pratique, le déploiement des

[791] Mendoza-Caminade A., Le rôle du sous-traitant en matière de données personnelles. In : Actes de colloques de l'IFR, Sécuriser la sous-traitance : quels nouveaux défis ? Presses de l'Université Toulouse 1 Capitole. pp. 103-115.

[792] Mendoza-Caminade A., Le rôle du sous-traitant en matière de données personnelles. In : Actes de colloques de l'IFR, Sécuriser la sous-traitance : quels nouveaux défis ? Presses de l'Université Toulouse 1 Capitole. pp. 103-115.

prestations de services cloud est, très souvent, externalisé dans un pays « tiers ». Il a pu être relevé deux types d'externalisation des services cloud connus sous l'appellation anglaise d' « offshoring » et de « nearshore »[793]. L'*offshoring* désigne la sous-traitance de certains services informatiques dans d'autres pays fortement éloignés du pays principal, autrement dit il s'agit de l'externalisation des services dans des pays lointains[794]. Le *nearshore* désigne au contraire la sous-traitance de certains services informatiques dans des pays proches du pays principal ; il s'agit, ici, d'une externalisation des services dans des pays proches[795]. Le sous-traitant sélectionné par le prestataire principal peut, également, être établi dans un pays éloigné de celui du client (situation appelée d'*offshoring*). Cette externalisation de services cloud dans un pays tiers engendre de facto une circulation des données. En présence d'une externalisation des services cloud dans un pays étranger, la question de la protection des personnes morales se pose. À cette fin, il est envisagé d'identifier quelles sont les règles applicables au transfert des données des personnes morales hors de l'Union européenne.

***357. L'absence de règles au transfert des données des personnes morales hors de l'Union européenne.*** Le RGPD prévoit des règles concernant la circulation des données hors de l'Union européenne, mais celles-ci s'appliquent uniquement aux données à caractère personnel[796]. En conséquence, les données à caractère non personnel ne peuvent pas bénéficier des règles de circulation des données hors de l'Union européenne édictées par le RGPD. Concernant le cadre légal de la circulation des données à caractère personnel hors de l'Union européenne, il existait déjà, avant l'adoption du RGPD, des réglementations spécifiques établissant les règles de protection[797], lesquelles ont été aujourd'hui renforcées par le RGPD[798]. Ces règles, de manière synthétique, exigent « un niveau de protection adéquat »[799] qui se caractérise par l'octroi au

[793] Sordet E., Milchior R., La définition des contours juridiques du cloud computing, Communication commerce électronique, novembre 2012.

[794] L'« offshoring » est défini comme : «la sous-traitance par l'externalisation de certaines activités préexistantes en France dans d'autres pays, en général fortement distants l'objet de cette opération est le plus souvent une réduction des coûts fiscaux financiers ou salariaux à l'image d'une délocalisation » : Sordet E., Milchior R., La définition des contours juridiques du cloud computing, Communication commerce électronique, novembre 2012.

[795] Le terme de « nearshore » désigne l'externalisation d'un service informatique vers des pays utilisant la même langue et situés dans un fuseau horaire identique ou proche Pour la France, le « nearshore » concerne les pays de l'Europe de l'Est et d'Afrique du Nord, l'offshore s'applique notamment à la Chine, à l'Inde et aux États-Unis : Sordet E., Milchior R.,, La définition des contours juridiques du cloud computing, Communication commerce électronique, novembre 2012.

[796] V. art. 2 paragraphe 1 du RGPD.

[797] V. *supra* n° 181.

[798] En particulier des règles définies au chapitre V du RGPD.

[799] V. article 44 du RGPD : « (..) toutes les dispositions du présent chapitre sont appliquées de manière que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis ».

profit du titulaire des données, de droits opposables[800], de voies de droit effectives[801]. En matière de données à caractère personnel, le cadre légal établi n'est pas une interdiction au transfert des données hors de l'Union européenne, mais impose le respect de certaines conditions[802]. Si l'on établit un comparatif, il en résulte que le transfert des données à caractère personnel hors de l'Union européenne est encadré par les règles spécifiques préexistantes au RGPD[803] alors que les données à caractère non personnel circulent librement sans cadre juridique et donc sans garanties légales.

***358.*** S'agissant du texte applicable aux données à caractère non personnel, il est spécifié au considérant 15 du RDNP que ce texte n'a pas vocation à s'appliquer « aux services de traitement des données ayant lieu en dehors de l'Union européenne ni aux exigences de localisation relatives à ces données »[804]. Cette disposition exclut, donc, du champ d'application du RDNP, les transferts de données réalisés hors de l'Union européenne. En raison de cette exclusion, il est considéré que ce texte est lacunaire. En effet, la question de la circulation des données dans le RDNP n'est envisagée que partiellement ; celle ayant lieu au sein de l'Union européenne. Or, il apparaît que les inquiétudes des personnes morales portent davantage sur la protection de leurs données lorsque celles-ci sont transférées hors des frontières de l'Union européenne. Aujourd'hui, il n'existe aucune réglementation spécifique encadrant le transfert des données des personnes morales hors de l'Union européenne. L'absence de règles concernant le transfert des données des personnes morales vers les pays tiers fait peser un risque quant à la protection des données des personnes morales. En conséquence, il existe une différence de protection légale entre les données à caractère personnel et les données des personnes morales. Cette différence de protection n'est pas justifiée dans la mesure que les transferts de données à caractère non personnel vers des pays tiers soulèvent de fortes inquiétudes, en particulier, concernant les données renfermant les secrets d'affaires et les droits de propriété intellectuelle[805]. Cette préoccupation a été prise en compte dans l'adoption récente du règlement européen intitulé acte sur la gouvernance des données qui établit un cadre pour autoriser le transfert de données à caractère non personnel vers des pays tiers.

---

[800] Le responsable du traitement doit informer la personne concernée des garanties appropriées ainsi que les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition. La délivrance de ces informations est une obligation positive à la charge des responsables du traitement des données : article 13 et 14 du RGPD.

[801] Exemples : le droit d'engager un recours administratif ou juridictionnel, d'introduire une action en réparation.

[802] V. *supra* n° 181.

[803] V. chapitre V du RGPD.

[804] Considérant 15 du RPDN.

[805] Petel A., Publication de l'Acte sur la gouvernance des données : les propositions de la Commission européenne, Revue Lamy Droit de l'Immatériel, N° 176, 1er décembre 2020.

***359.*** En outre, il apparaît que l'hégémonie étasunienne contribue à mettre en péril la protection des données des personnes morales françaises et européennes dans les contrats de cloud computing.

b) Une lacune légale face à l'hégémonie étatsunienne

***360. L'impact de l'hégémonie réglementaire et économique des États-Unis sur la protection des données.*** Aujourd'hui, le constat est que l'Union européenne est coincée entre les États-Unis et la Chine. Concernant les actions de l'Union européenne, certains auteurs ont affirmé que l'Union européenne « essaye de se mettre en selle dans l'économie du XXIe siècle, mais les résultats positifs de cette lutte âpre peinent à intervenir ; certaines autrices ont même pu dire que l'Europe est, sur ce chemin, « au milieu du gué »[806]. Le constat, aujourd'hui, est que l'effectivité du cadre légal de l'Union européenne semble difficile à mettre en œuvre dans un contexte international. Il apparaît nécessaire de protéger les clients, personnes morales, contre l'application du droit et des mesures à portée extraterritoriale. Le rapport Gauvain[807] fait état d'un protectionnisme judiciaire étasunien qui vient conforter notre observation initiale, celle d'une hégémonie réglementaire des États-Unis menaçant l'effectivité du cadre légal européen en matière de protection des données. Il mentionne la vulnérabilité des entreprises françaises face à l'hégémonie réglementaire des États-Unis et considère que « Les États-Unis d'Amérique ont entraîné le monde dans l'ère du protectionnisme judiciaire : alors que la règle de droit a, de tout temps, servi d'instrument de régulation, elle est devenue aujourd'hui une arme de destruction dans la guerre économique que mènent les États-Unis contre le reste du monde, y compris contre leurs alliés traditionnels et fidèles en Europe »[808]. Cette analyse permet de mettre en lumière le constat d'une hégémonie réglementaire étasunienne qui fragilise l'établissement et l'effectivité des règles européennes.

***361.*** Dans ce rapport, il est constaté que « les entreprises françaises ne disposent pas aujourd'hui des outils juridiques efficaces pour se défendre contre les actions judiciaires extraterritoriales engagées à leur égard, que ce soit par des concurrents ou par des autorités étrangères ». Ce rapport expose l'existence d'un rapport déséquilibré entre les États-Unis en position de domination réglementaire (par la mise en œuvre des lois sécuritaires) et économique (par des prestataires dominant le marché mondial de la data) et des clients « démunis » qui s'engagent dans un contrat d'adhésion. Sur ce point, la doctrine constate l'existence d'une fuite généralisée

[806] Favro K., Zolynski C., DSA, DMA : L'Europe encore au milieu du gué, Dalloz IP/IT 2021. 217.

[807] Gauvain R., Rapport parlementaire sur les procédures extraterritoriales, Revue Lamy droit des affaires, N° 157, 1er mars 2020).

[808] Ibid.

des données « en direction de ces personnes morales de droit américain »[809]. La domination économique étasunienne sur le marché de la data est réelle puisque, en effet, quelle entreprise ne ferait pas appel aux services de Google Cloud, d'AWS (Amazon), Microsoft One note pour stocker ses données dans le cloud[810].

***362.*** S'agissant de l'hégémonie réglementaire étasunienne, celle-ci est caractérisée par l'existence d'une prolifération de lois ayant une portée extraterritoriale[811]. À titre d'exemple, le Cloud Act permet « aux autorités judiciaires américaines d'obtenir des fournisseurs de stockage de données numériques (qui sont tous américains), sur la base d'un simple « warrant » (un simple mandat de perquisition), toutes les données non personnelles des personnes morales de toute nationalité, quel que soit le lieu où ces données sont stockées »[812]. Ce texte a, ainsi, suscité une inquiétude dans la pratique et des mises en garde par les autorités françaises ont été adressées aux entreprises. Dans ce contexte, le secrétaire d'État au Numérique, Mounir Mahjoubi, préconisait ainsi aux entreprises et aux institutions publiques de préférer, en matière de cloud, les prestataires français[813]. Cette préconisation ne peut plus être tenue concernant les données à caractère non personnel, depuis l'adoption du RDNP, puisque les principes sont la libre circulation des données et la prohibition des restrictions à la libre circulation des données au sein de l'Union européenne[814].

***363.*** Face à cette hégémonie réglementaire étasunienne, des auteurs ont pu considérer que « la prétention du droit européen à saisir des phénomènes qui dépassent ses frontières est battue en brèche, mais ce dernier se trouve incapable de « contrer » des offensives extraterritoriales du droit américain »[815]. Il en résulte de ce constat que « les lignes Maginot du droit européen se montrent bien incapables de prémunir leurs frontières contre les « intrusions digitales » de puissances étrangères » [816]. Il est, ainsi, mis en lumière que si le droit européen peut être protecteur pour les données, celui-ci pourrait ne pas s'appliquer lorsque les lois sécuritaires à portée extraterritoriale des États tiers sont mises en œuvre.

---

[809] Eggrickx B. et Jouffin E., *Cloud Act : nouvelle manifestation de l'extraterritorialité des textes US et réponse européenne,* Banque et Droit, hors-série, mars 2019.

[810] Ibid.

[811] V. *supra* n° 196 et suivants.

[812] Gauvain R., Rapport parlementaire sur les procédures extraterritoriales, Revue Lamy droit des affaires, Nº 157, 1er mars 2020).

[813] Eggrickx B. et Jouffin E., Cloud Act : nouvelle manifestation de l'extraterritorialité des textes US et réponse européenne, Banque et Droit, hors-série, mars 2019 : « le 3 juillet 2018, M. le secrétaire d'État au Numérique, Mounir Mahjoubi, préconisait ainsi aux entreprises et aux institutions publiques de préférer, en matière de cloud, les prestataires français »

[814] V. *supra* n° 326 et suivants.

[815] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279.

[816] Benabou V.-L., Le RGPD ou la ligne Maginot de la protection des données personnelles face aux acteurs extra-européens ? Rev. Mar. Un. Européen, 2021.

***364.*** Après avoir établi l'existence de lacunes légales dans le cadre de l'externalisation des services cloud à l'étranger, il est envisagé d'étudier les effets du vide juridique sur le contrat de cloud computing.

**2) Les effets du vide juridique sur la loi du contrat et la compétence juridictionnelle**

***365. Les principes de la détermination de la loi applicable et la compétence juridictionnelle.*** Lorsque la prestation d'hébergement des données est externalisée dans un pays éloigné de celui du client (situation de « offshoring »)[817], la question de la responsabilité du prestataire de service cloud se pose en cas d'atteinte aux données des personnes morales. Il apparaît que la détermination de la responsabilité dans une situation d'*offshoring* dépend de la loi applicable au contrat. Pour déterminer le régime légal et conventionnel de la responsabilité des parties au contrat, une attention sera, alors, portée aux clauses du contrat relatives à la loi applicable[818] et à la compétence juridictionnelle. L'identification de la réglementation applicable et la compétence juridictionnelle permettent de déterminer les droits des parties et en particulier le régime de la protection des données des personnes morales. De manière générale dans les contrats internationaux[819] conclus avec les professionnels, le principe est la liberté contractuelle appelée « principe d'autonomie » qui signifie que les parties sont libres de déterminer conventionnellement la loi qui s'appliquera au contrat ou précisément qui s'appliquera « au fond du contrat ». En droit international, « la loi applicable au fond du contrat (distincte le cas échéant de la loi applicable à la forme) est appelée lex contractus, ou simplement « loi du contrat » ; c'est la proper law »[820]. En revanche, en l'absence de choix des parties relatif à la détermination du droit applicable et/ou en présence d'un conflit de lois, c'est le règlement européen dit Rome I du 17 juin 2008[821] qui s'applique. Ce texte concerne la loi applicable aux obligations contractuelles et vise tous les types de contrats. Le principe d'autonomie est énoncé de manière expresse à l'article 3 dudit règlement[822]. Mais ce principe n'est pas absolu et dispose

[817] V. *supra* n° 355.

[818] Face à cette pratique « d'offshoring », la doctrine considère que « le fait de délocaliser hors de l'Union européenne l'informatique en nuage (cloud computing) entraine (..) des difficultés quant à la détermination du droit applicable » : Le Tourneau Ph., contrats du numérique, informatiques et électroniques, Dalloz, 12e édition, 2022-2023, p.463 n°342.15. V. également, Zolynski C., Quelle circulation des données non personnelles pour l'Union européenne ? revue des affaires européennes, 1er janvier 2018, numéro 1, page(s) 73-78.

[819] « Un contrat est international lorsqu'il comporte un élément d'extranéité, c'est-à-dire un élément extérieur significatif par rapport à l'ordre juridique à l'intérieur duquel on se place » : Testu F.X, Dalloz référence Contrats d'affaires, Chapitre 121 Traitement juridique des contrats internationaux, édition 2010.

[820] Testu F.X, Dalloz référence Contrats d'affaires, Chapitre 121 Traitement juridique des contrats internationaux, édition 2010.

[821] Règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (règlement Rome I).

[822] V. art. 3 du règlement Rome I du 17 juin 2008.

des limites pour certains types de contrats. À titre illustratif, ce principe d'autonomie connaît des limites pour le contrat de consommation[823], le contrat de travail[824] ainsi qu'en présence « de lois de police »[825], d'une « fraude »[826], et « d'une exception d'ordre public »[827].

***366.*** En l'absence de choix par les parties, le Règlement Rome I prévoit l'application de règles en fonction du type de contrat. À titre d'exemple, il est spécifié à l'article 4 que le contrat de vente est régi par la loi du pays dans lequel le vendeur a sa résidence habituelle; le contrat de prestation de services est régi par la loi du pays dans lequel le prestataire de service a sa résidence habituelle (cela comprend le contrat de prêt) ; le contrat portant sur la propriété intellectuelle est régi par la loi du pays dans lequel celui qui transfère ou concède les droits a sa résidence habituelle ; le contrat relatif à un immeuble (vente ou bail) est régi par la loi de situation de l'immeuble (avec une exception pour les baux de courte durée à une personne physique) ; le contrat de distribution ou de franchise est régi par la loi du pays dans lequel le distributeur a sa résidence habituelle[828]. En l'espèce, le contrat de cloud computing conclu entre des personnes morales est un contrat de prestation de services. En l'absence de choix des parties, la loi applicable au contrat est celle du pays dans lequel le prestataire de services a sa résidence habituelle[829].

***367.*** Quant au RDNP, il est précisé au considérant 16 que « le présent règlement ne fixe pas de règles relatives à la détermination de la loi applicable en matière commerciale et est donc sans préjudice du règlement (CE) no 593/2008 du Parlement européen et du Conseil[830]. Dès lors que la loi applicable à un contrat n'a pas été choisie conformément audit règlement, un contrat de prestation de services est en principe régi par la loi du pays dans lequel le prestataire de services à sa résidence habituelle »[831]. Si cette disposition mentionne expressément qu'elle ne fixe pas les

---

[823] V. art.6 règlement Rome I du 17 juin 2008.

[824] V. art.8 règlement Rome I du 17 juin 2008.

[825] Définition : « On désigne en droit international privé par l'expression loi de police (public policy rules, internationally mandatory law, overriding mandatory provisions…), les règles étatiques que leur but rend d'application nécessaire, même si le système juridique auquel ces règles appartiennent n'est pas désigné par la règle de conflit. Ce sont des lois fondamentales pour l'organisation politique, sociale ou économique du pays : elles ont un objet tel que l'État qui les a édictées estime indispensable de les voir appliquées aux situations présentant avec lui un rattachement significatif » : Testu F.X, Dalloz référence Contrats d'affaires, Chapitre 121 Traitement juridique des contrats internationaux, édition 2010.

[826] Définition : « La fraude est le fait de manipuler l'élément dont dépend la loi applicable pour obtenir un résultat défendu par la loi éludée, sans accepter les conséquences essentielles normalement attachées à ce choix » : Testu F.X, Dalloz référence Contrats d'affaires, Chapitre 121 Traitement juridique des contrats internationaux, édition 2010.

[827] Cette exception d'ordre public est prévue à l'article 21 du règlement Rome I : « L'application d'une disposition de la loi désignée par le présent règlement ne peut être écartée que si cette application est manifestement incompatible avec l'ordre public du for ». Précisément, « l'ordre public en cause n'est pas l'ordre public international constitué par les lois de police, mais l'ordre public du for au sens habituel, opposé à une application du droit étranger dont le principe est acquis » : Testu F.X, Dalloz référence Contrats d'affaires, Chapitre 121 Traitement juridique des contrats internationaux, édition 2010.

[828] Testu F.X, Dalloz référence Contrats d'affaires, Chapitre 121 Traitement juridique des contrats internationaux, édition 2010.

[829] Art. 4, paragraphe B du Règlement Rome I du 17 juin 2008.

[830] V. art. 3 du règlement Rome I du 17 juin 2008.

[831] Règle relative à la loi applicable à défaut de choix des parties au contrat.

règles relatives à la détermination de la loi applicable, elle rappelle du moins l'application de la règle prévue à l'article 4, paragraphe B du règlement européen dit « Rome I »[832].

***368.*** Concernant l'attribution de la compétence juridictionnelle en matière internationale, c'est le règlement européen dit Bruxelles I[833] qui s'applique et énonce un principe identique à celui défendu par l'article 42 du code de procédure civile français[834]. Le principe est le suivant : la compétence juridictionnelle est attribuée au tribunal du lieu où demeure le défendeur sauf volonté contraire des parties. Les parties peuvent décider de déroger à ce principe et fixer conventionnellement le tribunal compétent pour traiter le différend éventuel opposant les parties au contrat[835]. En l'occurrence, en cas d'atteinte aux données dans le cadre d'un contrat de cloud computing, le demandeur à l'action juridictionnelle est le client, personne morale, et le défendeur est le prestataire de services cloud.

***369.*** Il en résulte que si les parties n'ont pas prévu les clauses relatives au droit applicable et à la compétence juridictionnelle dans le contrat de cloud computing, le principe est, que la loi applicable et le juge compétent sont ceux du lieu d'établissement du prestataire de services cloud. L'application de ce principe légal n'est pas à l'avantage du client, personne morale. De la même manière, si le contrat de cloud computing conclu est un contrat d'adhésion, alors il est fort probable que les clauses soient rédigées en faveur du prestataire de services cloud et non du client, personne morale. Dans cette situation, le client français, personne morale, risque de connaître des actions judiciaires extraterritoriales d'autorités étrangères[836]. Compte tenu de ces règles, les questions du droit applicable et de la compétence juridictionnelle doivent susciter une attention particulière des parties au contrat. En matière délictuelle, la Cour d'appel a remis en question la jurisprudence traditionnelle de la Cour de cassation relative aux préjudices subis sur internet qui admettait « systématiquement » la compétence de la juridiction française dès lors que « les sites étrangers en cause sont accessibles depuis le territoire français »[837] dans l'affaire

---

[832] Règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (règlement Rome I).

[833] Règlement (UE) n°1215/2012 du Parlement européen et du Conseil du 12 décembre 2012, concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (également appelé règlement « Bruxelles I »), Il met à jour une loi de l'Union européenne (UE) relative à la compétence judiciaire, à la reconnaissance et à l'exécution des décisions en matière civile et commerciale (également appelée règlement « Bruxelles I»). Ce règlement vise à faciliter et à accélérer la circulation des décisions en matière civile et commerciale au sein de l'UE, conformément au principe de reconnaissance mutuelle et aux lignes directrices du programme de Stockholm : https://eur-lex.europa.eu/legal-content/fr/LSU/?uri=CELEX:32012R1215.

[834] Art. 42 du CPC : « 1. « Toute clause qui, directement ou indirectement, déroge aux règles de compétence territoriale est réputée non écrite à moins qu'elle n'ait été convenue entre des personnes ayant toutes contracté en qualité de commerçant et qu'elle n'ait été spécifiée de façon très apparente dans l'engagement de la partie à qui elle est opposée ».

[835] V. art. 25 du Règlement Bruxelles II.

[836] Gauvain R., Rapport parlementaire sur les procédures extraterritoriales, Revue Lamy droit des affaires, N° 157, 1er mars 2020.

[837] Mendoza-Caminade A., Internet et compétence juridictionnelle : (enfin) la fin de la compétence universelle du juge français, LPA 8 nov. 2007, n° PA 200722402 p.6.

Google contre Axa[838]. Elle « rejette clairement la compétence systématique du juge français découlant du critère de l'accessibilité au site internet, et elle subordonne cette compétence à la démonstration d'un préjudice réellement subi sur le territoire national »[839]. Il en résulte que le critère de l'accessibilité du site internet par des internautes en France est insuffisant pour reconnaitre la compétence du tribunal français. En effet, la simple « connexion au réseau ne doit plus permettre en tant que telle de justifier la compétence du juge français »[840]. Dans ce sens, elle avait déjà admis dans un arrêt précédent que « sauf à vouloir conférer systématiquement, dès lors que les faits ou actes incriminés ont eu pour support technique le réseau internet, une compétence territoriale aux juridictions françaises, il convient de rechercher et de caractériser, dans chaque cas particulier, un lien suffisant, substantiel ou significatif, entre ces faits ou actes et le dommage allégué »[841]. La Cour d'appel souligne la nécessité d'« une recherche approfondie du rattachement avec le dommage allégué »[842]. Il s'agirait ici de « rapporter la preuve d'un préjudice réel causé par le site internet »[843], c'est-à-dire de « démontrer un lien suffisant, substantiel ou significatif entre ces faits et le dommage allégué pour justifier de la compétence d'une juridiction française »[844]. Afin de prémunir le client contre l'application d'un droit étranger et la compétence étrangère d'une juridiction, il est conseillé de prévoir en amont de la signature du contrat de cloud computing les clauses relatives au droit applicable et à la compétence juridictionnelle[845]. Pour une illustration de propositions rédactionnelles de clauses relatives au droit applicable et à la compétence juridictionnelle, se référer aux développements de la deuxième partie consacrée au renforcement de la protection des données des personnes morales par l'ingénierie contractuelle.

[838] CA Paris, 6 juin 2007, n° 06-14890, Google contre Axa, RG n 06/14890.

[839] Mendoza-Caminade A., Internet et compétence juridictionnelle : (enfin) la fin de la compétence universelle du juge français, LPA 8 nov. 2007, n° PA 200722402 p.6.

[840] Ibid.

[841] CA Paris, 26 avril 2006, Comm. com. électr. 2006, comm. no 106, note Ch. Caron.

[842] Mendoza-Caminade A., Internet et compétence juridictionnelle : (enfin) la fin de la compétence universelle du juge français, LPA 8 nov. 2007, n° PA 200722402 p.6.

[843] Ibid.

[844] Ibid.

[845] Le Quellenec E., L'émergence d'un cloud souverain européen, Revue Lamy Droit de l'Immatériel, Nº 173, 1er août 2020.

***370. L'importance de la nationalité du prestataire et de la localisation des données sur le droit applicable et la compétence juridictionnelle***. En pratique, il apparaît que l'indication dans le contrat de cloud de computing d'une clause relative à l'application du droit de l'Union européenne ne suffit pas à garantir l'inapplication de la réglementation américaine dès lors que le prestataire de services de cloud computing est une société américaine ou que les données sont stockées dans des serveurs situés aux États-Unis. Un contrat peut avoir été formalisé sur le territoire de l'Union européenne entre une personne résidant sur ce même territoire et un prestataire de services cloud et malgré cela il y a un risque que les règles étasuniennes priment sur celles qui sont européennes. A titre illustratif de clause de localisation des données, le contrat cloud de la société OVH prévoit qu': « au moment de la création d'une Ressource, le Client choisit sa localisation parmi les Centres de données disponibles. Lorsque plusieurs localisations sont disponibles, le Client sélectionne celle(s) de son choix au moment de la Commande ». En l'espèce, la société OVH accorde au client, personne morale (à l'instar de la personne physique) la possibilité de choisir le lieu de la localisation du centre de données (datacenters) destiné à héberger ses données. En revanche, à la différence du contrat conclu avec un client, personne physique, il est spécifié qu'en choisissant un centre de données, « le Client reconnaît et accepte qu'il soit également soumis à la législation applicable sur le territoire sur lequel les Infrastructures sont installées et ses données stockées. Il reconnaît ainsi la faculté pour OVH cloud de suspendre son Service dès lors que celui-ci serait utilisé pour une activité prohibée sur le lieu de localisation physique des équipements fournis par OVH cloud »[846]. Cette clause informe, ainsi, le client que le choix de la localisation du centre de données a pour conséquence de soumettre le contrat à la loi du pays du lieu de situation du centre de données L'intégration de ce type de clause pourra ainsi, dans certains cas, rentrer en contradiction avec la clause relative au droit applicable. En outre, il apparaît que l'intégration d'une clause relative au droit applicable pourra être d'une efficacité limitée lorsque le prestataire de services cloud est une société américaine ou que les données sont stockées dans des serveurs situés aux États-Unis.

***371. Les propositions doctrinales pour contrer l'extraterritorialité judiciaire.*** Cette extraterritorialité judiciaire doit être prise en compte dans la réflexion de la mise en place de nouveaux outils juridiques pour sécuriser les données des personnes morales, en particulier, françaises et européennes. À ce titre dans le rapport Gauvain[847] , il est fait état de plusieurs recommandations et parmi elles, il propose d'établir une mesure « anti-cloud-act » afin de freiner l'action des « GAFA qui pourraient livrer les documents des entreprises françaises

[846] Ibid.

[847] Gauvain R., Rapport parlementaire sur les procédures extraterritoriales, Revue Lamy droit des affaires, N° 157, 1er mars 2020).

qu'elles détiennent aux autorités de poursuite américaines »[848]. Il semblerait qu'une telle proposition de mesure ne puisse pas être réalisable compte tenu de l'écosystème mondial favorable à une libéralisation des données[849]. Ensuite, il recommande « l'adoption d'une loi protégeant les entreprises françaises contre la transmission par les hébergeurs de leurs données numériques non personnelles aux autorités judiciaires étrangères »[850]. Cette loi serait, selon ce rapport, une sorte d'extension du RGPD aux données des personnes morales, qui permettrait de sanctionner les hébergeurs de données numériques qui transmettraient aux autorités étrangères des données non personnelles relatives à des personnes morales françaises en dehors des canaux de l'entraide administrative ou judiciaire. Malgré un fervent enthousiasme de certains auteurs concernant la mise en place d'un tel dispositif, il est considéré que la duplication du modèle du RGPD pour la protection des données des personnes morales serait inadaptée. Il serait plus opportun de créer une réglementation transnationale spécifique à la protection des données des personnes morales. Il est envisagé, dans la partie suivante, d'étudier les nouvelles propositions de mesures légales pour protéger les données des personnes dans le cadre d'un transfert de données hors de l'Union européenne[851].

***372. Un rapport contractuel déséquilibré au profit des prestataires.*** Lorsque ce ne sont pas les actes à portée extraterritoriale d'un État tiers, ce sont les fournisseurs eux-mêmes qui vont insérer une disposition qui leur est favorable et s'imposera au client, personne morale. Très souvent, le contrat conclu est un contrat d'adhésion. Dans ce sens, lorsqu'une personne morale française conclut en France un contrat de cloud computing avec une société américaine, telle que Microsoft, il est possible de constater que le contrat prévoit l'application du droit des États-Unis d'Amérique ainsi que la compétence juridictionnelle en faveur des juridictions américaines. À titre illustratif, dans le contrat cloud de Microsoft, il est stipulé que : « Le présent contrat est régi par les lois de l'État de Washington (États-Unis d'Amérique) sans donner d'effet aux dispositions régissant les conflits de lois, toutefois, (i) si vous êtes une entité publique américaine, le présent contrat est régi par les lois des États-Unis d'Amérique, et (ii) si vous êtes une entité publique fédérale ou locale aux États-Unis d'Amérique, le présent contrat est régi par les lois de l'État concerné. Toute action engagée pour faire appliquer le présent contrat doit être portée devant les tribunaux de l'État de Washington »[852]. Cette clause exclut, donc, formellement l'application des règles de conflits de lois et consacre l'application au

[848] Ibid.

[849] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279.

[850] Gauvain R., Rapport parlementaire sur les procédures extraterritoriales, Revue Lamy droit des affaires, N° 157, 1er mars 2020).

[851] V. *infra* n° 370 et suivants.

[852] Contrat Microsoft Cloud, article 9, j, page 8, MCA2017Agr(NA)(FRE)(Sep20172).

contrat du droit de l'État de Washington avec des exceptions réservées uniquement aux entités publiques américaines. En application de cette clause, le client, personne morale française, ne pourra pas opposer au prestataire de services cloud, l'application du droit français ni demander l'application des règles de conflits de lois. Dans ces conditions, cette clause permet de renforcer les droits du prestataire cloud américain puisque c'est le droit des États-Unis qui trouve à s'appliquer au contrat et attribue la compétence aux juridictions étasuniennes en cas de différend. Cette disposition nécessite la vigilance du client français, personne morale, puisqu'en cas de conclusion, il perd en plus de la maîtrise de ses données, la maîtrise pour régler son différend qui l'oppose à son prestataire. En l'espèce, la perte de maîtrise du règlement du différend se traduit par l'application du droit étranger et l'attribution de la compétence juridictionnelle aux tribunaux américains.

***373.*** En outre, cette clause témoigne de l'existence d'un rapport de force déséquilibré, lequel est exercé en faveur du prestataire de services cloud étranger. Dans ce cas de figure, le client s'engage à se conformer aux dispositions du contrat et accepte de soumettre le contrat aux règles des États-Unis. Alors, le postulat de départ d'une liberté contractuelle garante d'un contenu protecteur pour les parties trouve sa limite par ce déséquilibre de force existant entre les parties. Dans ce sens, laissez le soin aux acteurs de définir le cadre de leurs relations contractuelles, sans l'imposition de règles légales contraignantes, conforte l'idée d'un rapport de force contractuel déséquilibré et favorable aux fournisseurs de services cloud. Dans les autres cas de figure, c'est-à-dire hors hypothèse d'un contrat d'adhésion, nous pouvons dire que l'effectivité de la liberté contractuelle revient et dépendra de chaque « modèle de contrat » et de la capacité de négociation des parties prenantes au contrat[853] avec tout de même le maintien de la réserve relative à la mise en œuvre des actes à portée extraterritoriale, tels que les lois sécuritaires des États-Unis[854].

***374.*** À ce jour, les lacunes légales résident dans l'absence de règles pour transférer les données des personnes morales hors de l'Union européenne, mais ces lacunes pourront être compensées, dans une certaine mesure, en cas d'adoption d'une nouvelle réglementation.

[853] Eréséo N., Libre circulation des données et droit de la concurrence (à propos du règlement du 14 novembre 2018 relatif à la libre circulation des données non personnelles), Dalloz IP/IT 2020 p.414.

[854] V. *supra* n° 196 et suivants.

## B) Les palliatifs attendus dans le cadre d'un transfert hors de L'Union européenne

***375.*** Il est prévu d'étudier les dispositifs légaux proposés au niveau européen pour compenser l'existence d'un vide juridique en matière de protection des données des personnes morales dans le cadre d'un transfert hors de l'Union européenne. Ces dispositifs consistent en un contrôle du transfert des données par la Commission européenne (1) et par les juges (2).

### 1) Le contrôle du transfert des données par la Commission européenne

***376. Des palliatifs légaux, la mise en place d'un contrôle au transfert des données***. Au niveau européen, l'absence d'un cadre juridique au transfert des données à caractère non personnel a été prise en considération dans l'élaboration de la proposition d'Acte sur la Gouvernance des Données (« l'AGD ») publiée le 25 novembre 2020[855]. Pour remédier aux lacunes légales notamment en matière de transfert de données des personnes morales, l'AGD s'inscrit dans le cadre de la continuité de la création d'un marché unique des données et intègre la question du transfert des données à caractère non personnel vers des pays tiers. L'AGD met « l'accent sur les propriétés spécifiques des choses non-rivales, qui permettent d'envisager des modes d'échanges fondés sur la multiplication et non sur l'exclusivité »[856]. Pour pallier les lacunes légales existantes en matière de transfert des données hors de l'Union européenne, l'AGD propose plusieurs mesures.

***377.*** Afin d'assurer une protection des données à caractère non personnel dans le cadre des transferts et à l'instar du RGPD, l'AGD prévoit le contrôle de ces transferts. Il s'agirait de prévoir un contrôle des transferts de données à caractère non personnel hors de l'Union européenne sur le modèle de l'article 45 du RGPD relatif aux transferts fondés sur une décision d'adéquation[857]. L'AGD concilie ses règles avec celles du RGPD, en adaptant par exemple ses définitions ; à ce titre, « l'AGD distingue les « détenteurs des données » (personnes morales) et les « sujets de données » (individus) »[858]. L'objectif d'établir ce type de contrôle est de pouvoir garantir la protection de certaines données et en particulier celles qui renferment des secrets

[855] Proposition de Règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (Acte sur la gouvernance des données), 2020/0340 (COD), le 25 novembre 2020 : https://ec.europa.eu/transparency/regdoc/rep/1/2020/FR/COM-2020-767-F1-FR-MAIN-PART-1.PDF.

[856] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279.

[857] V. art. 45 du RGPD.

[858] Petel A., L'« Acte sur la gouvernance des données » : l'Union européenne dévoile le premier pilier du marché européen des données, La Semaine Juridique Edition Générale n° 22, 6 Juin 2022, 698.

d'affaires et des droits de la propriété intellectuelle[859]. La préoccupation initiale quant à la préservation des secrets d'affaires et des droits de la propriété intellectuelle est, ainsi, prise en compte dans ce texte. Pour autoriser ce transfert, des mécanismes de contrôles sont mis en place.

***378. Le contrôle du transfert de données par la Commission européenne***. Le mécanisme de ce contrôle se formaliserait par l'évaluation de la Commission européenne du système juridique du pays tiers concernant la protection des droits de la propriété intellectuelle et du secret d'affaires. Cette évaluation donne lieu à une décision d'adéquation dès lors qu'il est constaté que la protection dans le pays tiers est équivalente à celle de l'Union européenne[860]. À cet effet, pour évaluer le niveau de protection du pays tiers, il est pris en compte la législation applicable, l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes qui sont chargées dans le pays tiers d'assurer et de faire respecter le régime juridique de protection des données, l'existence de droits opposables et de voies de droits effectives[861]. Ce mécanisme de contrôle tel que décrit au considérant 15 de l'AGD est similaire à celui établi dans le cadre du RGPD dans la mesure où l'on retrouve les mêmes exigences notamment concernant la compatibilité avec le droit de l'Union européenne.

***379.*** La question se pose de savoir si un transfert de données à caractère non personnel vers un pays tiers peut avoir lieu en l'absence d'une décision d'adéquation de la Commission. Sur ce point, concernant le « réutilisateur de données »[862], il est précisé que ce dernier peut opérer le transfert des données vers un pays tiers dès lors qu'il s'engage à respecter les obligations prévues dans le règlement, et ce même après le transfert[863]. À titre illustratif, le *réutilisateur des données* devra « s'engager à respecter les règles européennes sur la propriété intellectuelle et les secrets d'affaires et qu'il reconnaisse la compétence des juridictions de l'UE pour tout litige relatif au respect de ces règles »[864]. Ces conditions pour autoriser le transfert des données à caractère non personnel hors de l'Union européenne sont communes dans le principe (exigence du respect de la réglementation européenne en la matière) aux conditions attachées au transfert des données à caractère personnel hors de l'Union européenne. La spécificité de ces conditions apparaît au niveau du champ de la protection ; en l'occurrence, ici, la propriété intellectuelle et

[859] V. considérant 13 de l'AGD.

[860] V. considérant 15 de l'AGD.

[861] Ibid.

[862] Le « réutilisateur de données » est défini comme « une personne physique ou morale qui dispose d'un accès licite à certaines données à caractère personnel ou non personnel et qui est autorisée à les utiliser à des fins commerciales ou non commerciales » : v. article 2 paragraphe 6 de l'AGD .

[863] V. considérant 16 de l'AGD.

[864] Petel A, Publication de l'Acte sur la gouvernance des données : les propositions de la Commission européenne, quels sont les points clés de la proposition d'Acte sur la gouvernance des données ? Revue Lamy Droit de l'Immatériel, N° 176, 1er décembre 2020.

les secrets d'affaires. En revanche, des conditions renforcées sont requises pour certains types de données telles que les données publiques à caractère non personnel « hautement sensibles »[865]. Pour ces données, il est précisé la possibilité de renforcer le niveau de protection par l'adoption de conditions supplémentaires telles que l'adoption d'actes délégués lesquels détermineront les conditions du transfert[866]. En définitive, il apparaît que ce dispositif de décision d'adéquation de la Commission européenne, proposé dans l'AGD, permettrait d'aboutir à un niveau de protection des données des personnes morales analogue à celui réservé dans le RGPD aux données à caractère personnel[867].

***380.*** Outre le dispositif de décision d'adéquation de la Commission européenne, l'AGD prévoit d'autres dispositifs, tels que les cas de demandes de transfert de données hors de l'Union européenne, par une autorité administrative ou judiciaire du pays tiers, fondées sur une législation étrangère.

**2) Le contrôle du transfert des données par les juges**

***381. Le contrôle du juge dans le cadre de l'application d'une loi étrangère.*** L'AGD a intégré la situation dans laquelle un transfert des données est exigé en application d'une législation étrangère. À ce titre, on songe à la réglementation américaine, avec la loi *FISA*[868] toujours d'application, laquelle accorde le droit aux États-Unis de demander aux opérateurs de transmettre les métadonnées des européens collectées depuis le territoire de l'Union européenne ou plus récemment le *Cloud Act*[869]. En réponse à l'adoption de ces législations sécuritaires américaines lesquelles permettent aux forces de l'ordre ou aux agences de renseignements américaines d'obtenir des opérateurs de télécommunications et des fournisseurs de services de Cloud computing des informations stockées sur leurs serveurs, que ces données soient situées aux États-Unis ou à l'étranger, la Commission européenne a prévu un dispositif défini dans l'AGD. Il est prévu le contrôle des juges pour autoriser le transfert de données qui a été demandé en application d'une loi étrangère. L'AGD énumère les conditions à remplir.

[865] Il est rappelé ici que « le qualificatif de « données sensible » employé par l'AGD est à distinguer des données dîtes « sensibles » au sens de l'article 9 du RGPD » : Petel A, Publication de l'Acte sur la gouvernance des données : les propositions de la Commission européenne, quels sont les points clés de la proposition d'Acte sur la gouvernance des données ? Revue Lamy Droit de l'Immatériel, Nº 176, 1er décembre 2020.

[866] Considérant 19 de l'AGD.

[867] Exemple : exigence d'une décision d'adéquation par la Commission prise sur le niveau de protection adéquat dans le pays tiers.

[868] V. *supra* n° 212 à 214.

[869] V. *supra* n° 211 à 213.

***382. Les conditions du transfert fondées sur une décision administrative ou judiciaire.*** L'AGD prévoit qu'en présence d'une décision administrative ou judiciaire d'un pays tiers qui exigerait un transfert de données à caractère non personnel, cette décision ne pourra être reconnue, ou rendue exécutoire que sous certaines conditions, lesquelles sont définies au considérant 17 dudit texte[870]. Pour qu'une décision soit reconnue, ou rendue exécutoire, il est exigé qu'elle soit fondée sur un accord international en vigueur dans ce pays tiers et dans l'UE, ou l'État membre concerné. Il s'agit de la première condition. Ensuite, si cette décision administrative ou judiciaire d'un pays tiers entraine un risque pour son destinataire d'être en contrariété avec le droit de l'UE ou de l'État membre concerné, alors il est précisé que ce transfert ne peut avoir lieu que si le système juridique du pays tiers présente certaines garanties telles que la publicité des motifs et de la proportionnalité de la décision, la possibilité de contester la décision devant une juridiction habilitée à apprécier les intérêts juridiques protégés[871]. En présence d'une telle décision administrative ou judiciaire, il existe deux possibilités : « Soit cette demande est fondée sur un accord international et elle doit être autorisée, soit elle ne l'est pas et elle doit alors être évaluée au regard des garanties juridiques qu'offre le pays tiers demandeur »[872].

***383.*** En définitive, en présence d'une demande de transfert des données hors de l'Union européenne par une autorité administrative ou judiciaire du pays tiers fondée sur une législation étrangère, il est exigé à titre de conditions, l'existence d'un accord international en vigueur dans ce pays tiers et dans l'UE ou l'État membre concerné. Puis en cas de risque d'une contradiction avec le droit de l'UE ou de l'État membre concerné, le transfert ne peut avoir lieu que si le système juridique du pays tiers présente certaines garanties juridiques (publicité des motifs, proportionnalité de la décision, recours contre la décision).

***384.*** En revanche, en dehors d'une demande de transfert fondée sur une décision administrative ou judiciaire, il est prévu qu'il incombe aux entités européennes de se prémunir contre le transfert international et l'accès des gouvernements aux données à caractère non personnel détenues dans l'Union s'ils sont susceptibles d'entrer en conflit avec les règles de l'Union européenne ou celles de l'État membre pertinent (par exemple en France, avec la loi n° 68-678 du 26 juillet 1968 dite de « loi de blocage » : JO 27 juill. 1968) »[873]. À titre illustratif, elles

[870] L'AGD, prévoit, également, la situation d'un cas d'un transfert de données dans un pays tiers lequel aurait pour conséquence d'être incompatible avec le droit de l'Union européenne et exige le respect d'une procédure de contrôle laquelle peut nécessiter l'intervention du juge.

[871] Publication de l'Acte sur la gouvernance des données : les propositions de la Commission européenne, extrait de la revue Lamy Droit de l'Immatériel, N° 176, 1er décembre 2020.

[872] Petel A., L'« Acte sur la gouvernance des données » : l'Union européenne dévoile le premier pilier du marché européen des données, La Semaine Juridique Edition Générale n° 22, 6 Juin 2022, 698.

[873] Ibid.

peuvent prévoir dans le contrat de cloud computing des dispositions qui encadrent les situations de transfert de données hors de l'Union européenne.

***385. L'importance des accords internationaux pour le transfert des données.*** Pour autoriser le transfert des données hors de l'Union en raison d'une décision administrative ou judiciaire européenne fondée sur une législation étrangère, il est exigé un accord international.[874] Or ces dernières années, les accords internationaux conclus entre l'Union européenne et les États-Unis ont été remis en cause. En particulier, l'accord dénommé *Privacy Shield* du 12 juillet 2016, lequel prévoyait un mécanisme de certification des opérateurs, a fait l'objet d'une invalidation dans deux décisions de la CJUE. À la suite de l'invalidation de l'accord Privacy Shield, la question s'est posée de savoir ce qu'il en sera des demandes de transfert des données vers les États-Unis par une autorité administrative ou judiciaire fondées sur la législation américaine. Pour répondre à cette question et si l'on se fie à la lettre de la disposition susvisée, la condition « d'un accord international » doit être remplie afin de reconnaître la force exécutoire d'une décision administrative ou judiciaire d'un pays tiers qui demanderait un transfert de données à caractère non personnel lesquelles sont couvertes par l'AGD. L'accord *Privacy Shield* ayant été invalidé, il ne peut être reconnu de force exécutoire à la décision administrative ou judiciaire des États-Unis qui demanderait un transfert de données à caractère non personnel. Pour permettre ce transfert, il sera nécessaire que l'Union européenne et les États-Unis établissent un nouvel accord international pour reconnaître la force exécutoire d'une décision administrative ou judiciaire des États-Unis demandant un transfert de données à caractère non personnel.

***386.*** La proposition d'Acte sur la Gouvernance des Données (« l'AGD ») a été adoptée par le Parlement européen et le Conseil de l'Union européenne le 30 mai 2022[875]. Le règlement européen maintient la protection de certaines données et en particulier celles qui renferment des secrets d'affaires et des droits de la propriété intellectuelle[876]. En revanche, les dispositifs du contrôle du transfert des données décrits dans l'AGD n'ont pas été repris en l'état, en particulier concernant le contrôle par la Commission[877]. Si l'on se réfère à l'article 31 du règlement européen sur la gouvernance des données qui traite de l'accès international et au transfert international, on s'aperçoit que le cadre est plus souple que celui proposé initialement dans l'AGD. A ce titre, il est rappelé le principe d'empêcher le transfert international de données à caractère non personnel ou l'accès international à ces données lorsque ce transfert ou cet accès

[874] V. *supra* n° 380.

[875] Règlement (UE) 2022/868 du parlement européen et du conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), publié au JOUE le 3 juin 2022, entré en vigueur le 23 juin 2022 et applicable effectivement à compter 24 septembre 2023 (délai de grâce). Ce texte établit un cadre général pour faciliter le partage des données au sein de l'Union européenne et prévoit des mécanismes de gouvernance.

[876] V. considérants 6, 10, 17 à 22 et art.3.1 du règlement européen sur la gouvernance des données.

[877] V. *supra* n° 375.

risque d'être en conflit avec le droit de l'Union ou le droit national de l'État membre concerné[878]. En présence d'une décision d'une juridiction d'un pays tiers ou d'une décision d'une autorité administrative d'un pays tiers exigeant le transfert des données à caractère non personnel détenues dans l'Union ou y donne accès, il est rappelé que celle-ci ne peut être reconnue ou rendue exécutoire qu'à la condition qu'elle soit fondée sur un accord international[879]. En l'absence d'accord international, le transfert de ces données ne pourra avoir lieu que si le système du pays tiers exige que les motifs et la proportionnalité de cette décision soient exposés et que cette décision revête un caractère spécifique, que l'objection motivée du destinataire peut faire l'objet d'un réexamen par une juridiction compétente du pays tiers et que la juridiction compétente du pays tiers est habilitée à prendre en compte les intérêts juridiques du fournisseur des données protégées par le droit de l'Union ou par le droit national de l'État membre concerné[880]. Dès lors que le transfert des données vers le pays tiers est autorisé, le règlement impose de fournir le volume minimal de données[881]. Il est, également, exigé d'informer, au préalable, le détenteur de données de l'existence d'une demande d'accès à des données le concernant émanant d'une autorité administrative d'un pays tiers sauf lorsque cette demande sert des fins répressives [882]. En outre, le règlement ajoute la possibilité pour la Commission européenne d'adopter des clauses contractuelles types en cas de transfert de données du secteur public vers des pays tiers. En définitive, il apparaît que ces dispositifs permettent de compenser le vide juridique existant en matière de protection des données des personnes morales dans le cadre d'un transfert hors de l'Union européenne. Par la même occasion ces dispositifs renforcent dans une certaine mesure la protection de ces données lorsqu'elles font l'objet d'un hébergement dans le cloud computing dans un pays éloigné.

[878] V. art. 31.1 du règlement européen sur la gouvernance des données.

[879] V. art. 31.2 du règlement européen sur la gouvernance des données.

[880] V. art. 31.3 du règlement européen sur la gouvernance des données.

[881] V. art. 31.4 du règlement européen sur la gouvernance des données.

[882] V. art. 31.4 du règlement européen sur la gouvernance des données.

## Conclusion du chapitre 2

***387.*** Cette partie a mis en lumière l'existence de lacunes légales en matière de transfert des données des personnes morales au sein de l'Union et hors de l'Union européenne. Le transfert de données au sein de l'Union européenne est réglementé par le règlement européen (RDNP) du 14 novembre 2018 qui établit un cadre applicable à la circulation des données à caractère non personnel dans l'Union européenne. Ce texte a consacré les principes de libre circulation des données à caractère non personnel dans l'Union européenne, l'interdiction des restrictions relatives à la localisation des données et un droit de portage. Ces mesures ont fait l'objet de vives critiques. Ce texte a été considéré comme lacunaire dans la mesure où il n'édicte que les règles relatives au transfert de données au sein de l'Union européenne et n'a pas vocation à traiter du transfert des données hors de l'Union européenne. Ce vide juridique a été pris en compte dans le cadre du règlement européen sur la gouvernance des données qui établit des dispositifs de protection des données non personnelles en matière de transfert de données de l'Union européenne vers un pays tiers. Ce cadre permet d'aboutir dans une certaine mesure à niveau de protection des données des personnes morales quasi analogue à celui réservé dans le RGPD aux données à caractère personnel.

# Conclusion titre 2

***388. L'existence de lacunes légales.*** Le questionnement de la protection des données des personnes morales dans le cadre de l'exécution d'un contrat de cloud computing trouve sa source dans le constat que les atteintes à la protection des données se sont accrues ces dernières années face au développement des NTIC. Cette partie a mis en lumière l'existence de lacunes légales en matière de protection des données des personnes morales dans les contrats de cloud computing. Il a été démontré que les lacunes légales résident, d'une part, dans l'inapplication des droits fondamentaux, de la réglementation générale de la protection des données à caractère personnel et d'autre part, dans l'absence d'une réglementation spécifique à la protection des données des personnes morales dans le cloud. Il est observé que ces lacunes légales impactent directement la protection des données des personnes morales dans les contrats de cloud computing. Ces impacts sont perceptibles dans le contrat de cloud computing avec la constatation de déséquilibres contractuels et de situations d'abus de dépendance économique. En raison de ces lacunes légales, les personnes morales doivent, donc, considérer avec attention le contenu des dispositions du contrat de cloud computing et proposer l'intégration de clauses garantissant la protection de leurs données.

***389. L'absence de cadre légal pour le transfert de données hors de l'Union européenne.*** Le RDNP qui réglemente le transfert des données à caractère non personnel est lacunaire dans la mesure où il n'édicte que les règles relatives au transfert de données au sein de l'Union européenne et n'a pas vocation à traiter du transfert de données hors de l'Union européenne. En conséquence, ce texte ne permet pas de pallier l'existence du vide juridique quant à l'encadrement du transfert des données hors de l'Union européenne. L'existence de ce vide juridique suscite les inquiétudes des clients, personnes morales. Afin de se prémunir contre les risques d'une perte de contrôle sur les données et sur la procédure juridictionnelle en cas de différend, l'ingénierie contractuelle est mise en œuvre du moins lorsque celle-ci est envisageable (hors contrat d'adhésion). Ce vide juridique a été pris en compte dans le cadre du règlement européen sur la gouvernance qui intègre la question du transfert hors de l'Union européenne pour renforcer la protection des données confidentielles des personnes morales sur un modèle se rapprochant de celui des personnes physiques.

# Conclusion partie 1

***390. Les lacunes légales pour la protection des données à caractère personnel.*** Le RGPD s'applique au contrat cloud dès lors qu'il contient une clause de collecte et de traitement des données à caractère personnel. Or, l'intégration d'une telle clause est critiquable au regard de la nature et de l'objet du contrat cloud et compte tenu du déséquilibre contractuel existant entre les parties au contrat cloud. Il a été présenté, dans cette partie, l'idée « d'une forme de dépossession invisible des données à caractère personnel » de l'utilisateur (personne physique) portant, ainsi, atteinte au droit fondamental à la protection des données à caractère personnel et au droit à la vie privée. La protection des données à caractère personnel est remise en cause dans le cadre d'un transfert des données en dehors de l'Union européenne ; en particulier lorsque le transfert s'opère vers les États-Unis. Il est constaté que les lois sécuritaires américaines ont une incidence directe quant à l'effectivité des règles européennes en raison de la primauté des premières sur les secondes. Il a été considéré que le texte européen (RGPD) relatif à la protection des données à caractère personnel demeure lacunaire, d'une part, face aux États-Unis lorsqu'ils décident de mettre en œuvre leurs lois sécuritaires pour récupérer les données de résidants européens et d'autre part, en présence de montages contractuels opérés par les fournisseurs de services cloud. Certains prestataires de services cloud ont procédé à des montages contractuels afin d'être en conformité aux obligations du RGPD sans pour autant aboutir à une protection effective des données à caractère personnel. Face à ce montage contractuel, il a été proposé d'accorder une vigilance particulière des clauses relatives au traitement des données (identification des données), au droit applicable, à la localisation des serveurs. Malgré cette vigilance, il apparaît que l'intégration de ces clauses au contrat ne suffisait pas à garantir l'inapplication de la réglementation américaine dès lors que les données sont stockées dans les serveurs d'une société américaine et de ses filiales européennes (situées aux États-Unis ou hors des États-Unis). En revanche, la clause de localisation des serveurs sur le territoire de l'Union européenne garde son utilité vis-à-vis des sociétés européennes lorsqu'elles s'engagent à stocker les données des utilisateurs dans des serveurs localisés au niveau national ou de l'Union européenne et s'interdisent de les stocker et de transférer les données dans des serveurs localisés hors de l'Union européenne et en particulier aux États-Unis.

***391. L'existence de lacunes légales en matière de protection des données des personnes morales dans le cadre d'un contrat de cloud computing.*** Les lacunes légales de la protection des données des personnes morales résident dans l'inapplication des droits fondamentaux, de l'inapplication de la réglementation générale de la protection des données à caractère personnel,

de l'absence d'une réglementation spécifique à la protection des données des personnes morales dans le cloud. Il a été constaté que ces lacunes légales ont contribué au renforcement de la perte de contrôle de la personne morale sur les données et ont un impact direct en matière contractuelle dans l'établissement des droits et des obligations des parties. En raison de ces lacunes légales, les personnes morales doivent accorder une vigilance particulière au contenu des dispositions du contrat du contrat de cloud computing. Quant au transfert des données des personnes morales, c'est le RDNP qui s'applique, mais ce texte est lacunaire en raison qu'il ne réglemente pas le transfert de données hors de l'Union européenne. Ce vide juridique en matière de transfert de données hors de l'Union européenne suscite les inquiétudes quant à la sécurité, la confidentialité, l'intégrité des données et la qualité de service. Pour minimiser ces risques, il a été proposé d'accorder une vigilance aux clauses relatives à la localisation des serveurs, au transfert des données et au droit applicable. Outre les précautions contractuelles, l'adoption récente du règlement européen sur la gouvernance des données permet de contribuer, dans une certaine mesure, au renforcement de la protection des données des personnes morales en particulier dans le cadre d'un transfert de données de certaines données des personnes morales de l'Union européenne vers un pays tiers.

***392.*** Après avoir étudié les lacunes légales en matière de protection des données à caractère personnel et des données des personnes morales, l'objet de la partie suivante porte sur l'étude du renforcement de la protection des données dans les contrats de cloud computing.

# Partie 2 : Les renforcements de la protection des données dans les contrats de cloud computing

***393. La prise en compte par le droit des spécificités du cloud computing.*** Pour prétendre à une protection juridique effective des données dans les contrats de cloud computing, faudrait-il en amont que le droit puisse se saisir des spécificités de la technologie du cloud ? L'élaboration de régimes juridiques doit considérer d'une part, les spécificités techniques du cloud et d'autre part, le contexte de la mondialisation. Les données dans « le nuage » circulent librement sans tenir compte des frontières étatiques, sans se soucier des droits des personnes concernées et sans réel contrôle sur les flux de données. À la suite de l'étude entreprise en première partie, le droit positif doit poursuivre ses efforts d'adaptation aux NTIC et en particulier à la technologie du cloud. Le droit positif nécessite d'être encore plus en phase avec les besoins de protection des utilisateurs du cloud computing. Sur le besoin de protection des données, la doctrine souligne que « ce mouvement d'intensification des échanges de données crée des sources de valeurs nouvelles, mais fait également naître des risques inédits (notamment pour la tranquillité des personnes, et la sécurité des organisations ainsi que celles de leurs actifs, et de leur réputation). Comme à chaque période de transformation, le droit a été convoqué pour encadrer cette "transformation numérique" (..) »[883]. La question de la protection des données des utilisateurs des NTIC n'est pas nouvelle, le droit s'en est saisi depuis la naissance d'internet. Un cadre juridique s'est progressivement développé au fil des années. La question est de savoir si la réponse du droit est, aujourd'hui, suffisante pour assurer un niveau adéquat de protection des données des personnes parties à un contrat de cloud computing.

***394. La nécessité d'un cadre spécifique***. La mise en place d'un cadre légal spécifique à la protection des données dans le cloud devra sans doute surmonter la principale difficulté consistant à trouver un équilibre entre d'une part, la protection des données et d'autre part la préservation des libertés et en particulier « la liberté de commerce et d'industrie ». Concernant la réglementation applicable au cloud computing, il n'existe pas, en France et en Europe, un régime juridique spécifique à la protection des données dans le cloud computing, mais un corpus de règles en évolution sur des catégories de données, lesquelles ont pu être appréhendées en première partie. Partant de la constatation qu'il existe des lacunes légales en matière de protection des données dans les contrats de cloud computing, l'objectif est d'envisager les

[883] Bourgeois M., JurisClasseur Communication, Fasc. 962 : cloud computing – Les défis contractuels du Cloud Computing, 1er mai 2020.

moyens juridiques permettant de remédier (même partiellement) à ces lacunes et renforcer, ainsi, la protection des données dans les contrats de cloud computing. Afin d'aboutir à une protection effective de la protection des données, il ne suffit pas de consacrer des droits ou d'identifier des atteintes, mais aussi d'observer quelle est l'application concrète de ces textes, en particulier en matière de responsabilité et de réparation du préjudice subi.

***395. L'étude du renforcement de la protection des données à caractère personnel***. Compte tenu de l'absence d'un régime spécifique à la protection des données dans le cloud computing[884], il convient ici d'étudier les moyens juridiques permettant de renforcer la protection des données dans les contrats de cloud computing. Le renforcement de la protection des données à caractère personnel se traduit par la mise en œuvre de droits liés à la titularité des données et en particulier la notion d'un droit à la propriété des données et du droit à l'autodétermination informationnelle. S'agissant des moyens juridiques permettant un renforcement des droits des personnes physiques, il est envisagé de mener une réflexion sur l'élargissement du champ de la réparation et des responsabilités.

***396. L'étude du renforcement de la protection des données des personnes morales.*** À l'instar des personnes physiques, les personnes morales ne disposent pas d'une réglementation spécifique à la protection de leurs données dans les contrats de cloud computing. Il est proposé d'étudier la loi et le contrat de cloud computing pour renforcer la protection des données des personnes morales dans les contrats de cloud computing.

***397.*** **Plan de la Partie 2** : Cette partie est consacrée à l'étude du renforcement de la protection des données à caractère personnel (**Titre 1**) et des données des personnes morales (**Titre 2**).

[884] Quéméner M., Dalle F., Wierre C., Quels droits face aux innovations numériques, Gualino, Lextenso, 2020.

# Titre 1 : Les renforcements de la protection des données à caractère personnel

***398.*** ***La nécessité d'un renforcement des données à caractère personnel***. Il a été observé en première partie l'existence de lacunes légales pour la protection des données à caractère personnel en raison notamment de l'absence d'un régime spécifique[885] ainsi que l'existence de failles technologiques pouvant impacter directement la sécurité des données dans le cadre de l'exécution des contrats de cloud computing. Il apparaît, donc, nécessaire d'envisager les moyens juridiques pour renforcer la protection des données à caractère personnel dans les contrats de cloud computing. Il convient, tout d'abord, d'étudier la mise en œuvre de droits liés à la titularité des données et spécifiquement, la notion d'un droit à la propriété des données et l'effectivité du droit à l'autodétermination informationnelle dans les contrats de cloud computing. Puis, il est envisagé d'engager une réflexion sur le droit à la réparation au profit des personnes physiques en cas d'atteinte au droit à la protection des données à caractère personnel et au droit à la vie privée.

***399.*** **Plan du Titre 1** : Le renforcement de la protection des données à caractère personnel dans les contrats de cloud computing est appréhendé par l'application des droits attachés à la titularité des données (Chapitre 1) et au droit à la réparation (Chapitre 2).

[885] Ibid.

# Chapitre 1 : Le renforcement par les droits liés à la titularité des données

***400. L'identification des moyens juridiques pour le renforcement des données.*** En raison de l'absence d'une réglementation spécifique à la protection des données à caractère personnel en matière de cloud computing[886], il est question de proposer dans ce chapitre les moyens juridiques permettant de renforcer la protection des données à caractère personnel dans les contrats de cloud computing. Ce chapitre étudie le droit à la propriété des données et le droit à l'autodétermination informationnelle. Concernant le droit de propriété, l'on s'interroge sur la pertinence de consacrer « un droit de propriété des données » pour renforcer la protection des données à caractère personnel dans les contrats de cloud computing. S'agissant du droit à l'autodétermination informationnelle, il s'agit d'étudier son cadre légal afin d'envisager sa transposition pour une protection effective des données dans les contrats de cloud computing.

***401.*** **Plan.** Le renforcement de la protection des données à caractère personnel dans les contrats de cloud computing est appréhendé par la notion du droit de propriété des données (**Section 1**) et par le droit à l'autodétermination informationnelle (**Section 2**).

## Section 1 : La proposition d'une protection des données par le droit de propriété

***402.*** La volonté de certains auteurs de consacrer un droit de propriété semble rentrer en conflit avec celle l'Union européenne qui accorde à la liberté des échanges et du commerce une valeur tout aussi importante qu'à celle de la protection des données à caractère personnel. Ce constat se fonde, notamment, sur l'intitulé du RGPD[887] qui place au même niveau « la protection des données » et « la libre circulation des données ». En revanche, le droit de propriété demeure plébiscité par certains pour protéger les données de la personne physique[888].

***403.*** **Plan.** Pour appréhender la proposition d'un droit de propriété des données, il est envisagé d'étudier l'application des caractéristiques légales du droit de propriété au titulaire des données à caractère personnel (A) ainsi que l'attrait pour le droit de « propriété » comme moyen de protection des données à caractère personnel (B).

---

[886] V. *supra* n° 84.

[887] Les art. 6 Loi informatique et libertés (*op. cit.*) et art. 9 al. 1 du RGPD posent le principe d'interdiction de traitement des données sensibles sauf exceptions prévues par les textes.

[888] V. *infra* n° 413 et suivants.

## A) L'application légale d'un droit de propriété des données

***404.*** **Plan.** La question est de savoir si la propriété telle qu'appréhendée en droit positif est la réponse adéquate à la protection des données dans les contrats cloud. Il est envisagé d'étudier les caractéristiques légales du droit de propriété (1) suivi de l'application des attributs de la propriété au titulaire des données à caractère personnel (2).

### 1) Les caractéristiques légales du droit de propriété

***405.*** ***La thèse de la patrimonialisation des données.*** Ces auteurs, plébiscitant un droit de propriété des données des personnes physiques, fondent leurs thèses sur une analyse patrimoniale du droit à la protection des données personnelles[889]. Selon, G. Koenig, le président de Génération libre, estime en effet qu'« il s'agit de rendre aux citoyens ce qui leur appartient. (..) Car si les données sont, selon la formule convenue, le pétrole du 21e siècle, il est temps de poser la question : à qui appartient le pétrole? Au producteur primaire, qui le revend à d'autres pour le raffinage. C'est-à-dire à vous et à moi, producteurs de données, qui devrions être rémunérés pour la matière première que nous pourvoyons aux algorithmes du Big Data. »[890]. Une telle proposition s'inscrit dans une quête de rééquilibrage des pouvoirs entre prestataires et clients et donc d'un renforcement des droits de la personne physique pour protéger ses données personnelles. En revanche, est-ce qu'une telle proposition fondée sur la patrimonialisation des données, et donc d'une propriété des données, est la solution pertinente au niveau juridique pour renforcer de manière effective la protection des données dans les contrats de cloud computing.

***406.*** Avant d'envisager la concrétisation d'un droit de propriété des données des personnes physiques, il convient de définir les caractéristiques légales de la propriété.

***407.*** ***Les définitions de la propriété***. Concernant la terminologie du droit à la propriété, « la définition du droit de propriété de l'économiste diffère de celle du juriste. Le premier conçoit le droit de propriété comme un droit d'usage alors que le second le conçoit comme un droit de possession »[891]. Le rapprochement entre le droit de propriété et le droit de possession provient

[889] Castex L., « Les éternités numériques un essai d'analyse prospective », RLDI 2016/11, p. 49, spéc. II ; Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi. Pour une patrimonialité des données personnelles, Rapport du Collectif génération libre, L. Léger (Dir.), janv. 2018, <https://www.generationlibre.eu/data-a-moi/>, spéc. p. 116-20 proposant la mise à disposition des données par des smartcontracts usant de signatures électroniques et blockchain ; dans Netter E., Ndior V., Puyraimond J-F, Vergnolle S. Regards sur le nouveau droit des données personnelles. Centre de droit privé et de sciences criminelles d'Amiens. 2019, 979-10-97323-05-9. hal-02357967.

[890] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Rapport (sous la direction de Léger L.), Mes data sont à moi - Pour une patrimonialité des données personnelles, janvier 2018 : https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf.

[891] Fabrice Rochelandet, Économie des données personnelles et de la vie privée, La découverte, 2010.

du principe civil qu'« en fait de meubles, possession vaut titre »[892] ; ce qui signifie qu'en matière mobilière, la possession vaut titre de propriété. En réalité, ces deux notions se complètent et s'opposent à la fois : la propriété est un pouvoir de droit sur la chose ; alors que la possession est un pouvoir de fait sur la chose[893]. En droit civil français, la propriété est définie à l'article 544 du Code civil comme « le droit de jouir et de disposer des choses de la manière la plus absolue, pourvu qu'on n'en fasse pas un usage prohibé par les lois ou les règlements ». La propriété, ainsi, définie, concerne les meubles et les immeubles. Le droit de propriété est un droit fondamental affirmé aux articles 2[894] (droit naturel et imprescriptible) et 17[895] (un droit inviolable et sacré) de la Déclaration des droits de l'homme et du citoyen (DDHC). La propriété a pour caractères d'être d'un droit absolu, perpétuel et exclusif. Un droit absolu signifie qu'aucune personne ne peut porter atteinte à la propriété (article 544 du code civil) sauf cas prévus par la loi ou les règlements. Le droit de propriété est perpétuel, c'est-à-dire, qu'il existe aussi longtemps que la chose sur laquelle il porte, existe et se transmet aux héritiers au décès du propriétaire. Un droit exclusif signifie qu'aucune autre personne ne puisse exercer des droits sur la chose objet de la propriété ; autrement dit, la propriété s'exerce sans l'entremise d'une autre personne. La propriété est opposable *erga omnes*, c'est-à-dire à l'égard de tous. Outre ces caractères, le droit de propriété dispose de trois attributs fondamentaux[896] qui sont l'*usus* (le droit d'utiliser la chose), le *fructus* (le droit de disposer les fruits de la chose) et l'*abusus* (le droit de disposer de la chose). L'*usus* correspond au droit d'utiliser la chose et de contrôler l'utilisation de la chose, ainsi que la faculté de reprendre possession de la chose. Le *fructus* est le droit de disposer les fruits de la chose, c'est-à-dire de tous les profits de la chose (exemples : un loyer, un revenu). L'*abusus* est le droit de disposer de la chose, ce qui signifie que le propriétaire a la faculté de détruire la chose et de transférer la propriété par cession, échange ou donation. Il s'agit, ainsi, des caractéristiques légales attendues lorsque l'on envisage la propriété au sens juridique du terme, est-ce que ces caractéristiques peuvent être transposable en matière de données à caractère personnel ?

---

[892] Art. 2276 du code civil.

[893] Karamani-Pelacuer F., Gougot L., La propriété et la possession, fiche pratique n°3209, Lexis360, 3 février 2020.

[894] Déclaration des Droits de l'Homme et du Citoyen de 1789, art. 2 : « Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression ».

[895] Déclaration des Droits de l'Homme et du Citoyen de 1789, art. 17 « La propriété étant un droit inviolable et sacré, nul ne peut en être privé, si ce n'est lorsque la nécessité publique, légalement constatée, l'exige évidemment, et sous la condition d'une juste et préalable indemnité ».

[896] V. *supra* n° 402.

***408.*** Il convient pour répondre à la question d'étudier, à présent, si ces attributs peuvent s'appliquer au profit de la personne physique sur ses données à caractère personnel.

**2) L'application des attributs de la propriété au titulaire des données à caractère personnel**

***409. La détermination de l'usus dans le rapport entre la personne physique et sa donnée à caractère personnel.*** Juridiquement, « les données » sont des biens meubles[897] et ce en application de l'article 528 du Code civil qui dispose que : « sont meubles par leur nature les biens qui peuvent se transporter d'un lieu à un autre ». Les données sont des biens meubles pouvant être qualifiés d'incorporels puisqu'un bien meuble incorporel est défini « par opposition aux biens corporels qui sont des biens tangibles[898]. Les biens incorporels « ont pour dénominateur commun de ne comporter aucune matière »[899]. La reconnaissance des meubles incorporels est issue « d'une opération intellectuelle, abstraite »[900]. En conséquence, si les données sont des biens meubles incorporels alors l'exercice d'un droit réel direct sur la chose ne pourra pas être réalisé. En effet, le droit réel est « un droit qui donne à la personne un pouvoir direct et immédiat sur une chose et ce pouvoir s'exerce sans l'entremise d'un autre individu »[901]. La donnée étant un bien incorporel, il s'agit, alors, d'envisager l'exercice « d'un droit personnel sur l'usage de la chose ». Le droit personnel ou "droit de créance" est une notion juridique qui la distingue du "droit réel" ; « il s'agit d'une relation établie entre deux ou plusieurs personnes, de sorte qu'en exécution de la convention qu'elles ont établie entre elles l'une ou l'autre sont contraintes à exécuter des prestations convenues au profit des autres »[902]. De manière plus succincte, le droit personnel est « le pouvoir d'une personne d'exiger d'une autre qu'elle donne, fasse ou ne fasse pas quelque chose »[903]. Dans son sens commun, l'usage correspond à l'action de se servir ou utiliser une chose. En termes juridiques, le droit d'usage ou l'*usus* est une des prérogatives accordées au propriétaire. Cette prérogative confère au propriétaire un droit personnel d'utiliser la chose. Le droit d'usage est un droit personnel qui contrairement à l'usufruit est un droit réel permettant à l'usufruitier d'exercer directement des droits sur la

[897] V. art. 527 du code civil : « Les biens sont meubles par leur nature ou par la détermination de la loi ». Également, v. art. 528 « Sont meubles par leur nature les biens qui peuvent se transporter d'un lieu à un autre ».

[898] Chadelat C., Valdès-Boulouque M., Mission d'évaluation du dispositif législatif et réglementaire des ventes volontaires de meubles aux enchères publiques, déc. 2014, p. 30.

[899] Ibid.

[900] Ibid.

[901] Karamani-Pelacuer F., Gougot L., La propriété et la possession, fiche pratique n°3209, Lexis360, 3 février 2020.

[902] Définition du droit personnel, dictionnaire juridique de Serge Braudo, 1996-2022 : https://www.dictionnaire-juridique.com/definition/droit-personnel.php.

[903] Karamani-Pelacuer F., Gougot L., La propriété et la possession, fiche pratique n°3209, Lexis360, 3 février 2020.

chose[904]. En cas de démembrement de la propriété, le titulaire du droit d'usage à l'inverse du propriétaire ne dispose pas du *fructus* (le droit de disposer des fruits) ou de l'*abusus* (le droit de disposer de la chose). En matière de données à caractère personnel, le droit d'usage appartient « au titulaire » de la donnée personnelle (la personne physique identifiée par cette donnée) et peut décider de « transférer » son droit d'usage au prestataire de services cloud. En définitive, il apparaît que la personne physique dispose bien de l'*usus* sur sa donnée à caractère personnel ainsi que la faculté de transférer son droit d'usage au prestataire de services. Elle dispose, donc, du premier attribut dont jouit un propriétaire au sens civil du terme. Qu'en est-il du *fructus* ?

***410. La détermination du fructus dans le rapport entre la personne physique et sa donnée à caractère personnel.*** Si le titulaire des données a un droit d'usage sur ses données à caractère personnel, il apparaît en pratique que celui qui tire les bénéfices « d'un droit d'usage » (droit de disposer des fruits de la chose), au travers d'une licence de collecte et de traitement des données prévue au contrat de cloud computing, n'est pas le titulaire de la donnée lui-même, mais le prestataire de services cloud. En application de cette clause, l'utilisateur des services cloud, accorde au prestataire de services cloud une autorisation d'utiliser les données stockées dans le cloud (droit d'usage temporaire). En pratique, ce transfert du droit d'usage des données est accordé gratuitement ; on parle alors de « free data ». Dans ce schéma, c'est la personne physique (titulaire de la donnée) qui va consentir au profit du prestataire de services cloud une licence d'utilisation (droit d'usage) des données dans un cadre préalablement défini au sein du contrat de cloud computing (exemple : autorisation d'utiliser les données pour l'amélioration des services cloud ou de l'expérience client). À titre illustratif, il est repris, ci-après, une clause dans les conditions du contrat cloud de Google qui accorde un droit d'usage des données stockées dans le cloud : « Lorsque vous importez, soumettez, stockez, envoyez ou recevez des contenus à ou à travers nos Services, vous accordez à Google (et à toute personne travaillant avec Google) une licence, dans le monde entier, d'utilisation, d'hébergement, de stockage, de reproduction, de modification, de création d'œuvres dérivées (…) »[905].

***411.*** Dans cette configuration, il serait utile de pouvoir renverser cette situation au profit de l'utilisateur du service cloud (titulaire de la donnée à caractère personnel) en consacrant une obligation de contrepartie à cette autorisation du droit d'usage des données. Sur ce point, le prestataire de services cloud peut rétorquer qu'il existe déjà une contrepartie qui résiderait dans l'utilisation par le titulaire des données d'un service cloud gratuit. Par conséquent, dès lors que

[904] Ainsi l'usufruitier à la possibilité de de céder son droit d'usufruit, de le transmettre éventuellement à titre gratuit, voire de l'hypothéquer.

[905] Clause figurant dans les conditions du contrat cloud de Google : https://policies.google.com/terms.

le titulaire des données bénéficie d'un service de cloud gratuit, la condition de « contrepartie » à la licence du droit d'usage des données serait remplie. Il revient, donc, à l'utilisateur du service cloud d'accorder une attention particulière à la clause relative à la licence du droit d'usage. Il est possible de considérer que dans le cadre d'un contrat de cloud computing gratuit, la détermination du *fructus* de la personne physique résiderait dans l'accès et l'utilisation des services de cloud computing. En conséquence, la personne physique dispose d'un *fructus* sur ses données dans le cadre d'un contrat de cloud computing de services de cloud computing.

***412.*** L'analyse d'une propriété des données ne s'arrête pas avec l'étude de l'*usus* et du *fructus*, elle se poursuit avec l'analyse de l'*abusus* (droit de disposer de la chose).

***413. La détermination de l'abusus dans le rapport entre la personne physique et sa donnée à caractère personnel.*** Malgré la consécration par les textes d'un droit de contrôle sur l'usage des données personnelles[906], aucun texte ne confère à la personne physique un *abusus* sur les données personnelles, entendues comme la capacité à disposer de la chose, c'est-à-dire la faculté de détruire la chose et de transférer la propriété par cession, échange ou donation. Les données numériques personnelles ne sont pas reconnues en l'état comme des « biens » pouvant faire l'objet d'une appropriation. La protection des données à caractère personnel est un droit fondamental[907] attaché à la personne et comme tous les droits de la personnalité, ils sont inaliénables. Un droit inaliénable est un droit inhérent à un individu du seul fait de ce qu'il est (condition humaine), il ne peut être ni transmis, ni cédé, ni vendu et s'éteint au décès de la personne qui le détient[908]. La personne physique n'est pas autorisée par la loi à céder à titre onéreux ou à titre gratuit ses données à caractère personnel ; il s'agit de « biens immatériels » hors du commerce[909] dans le sens où elles ne peuvent pas faire être vendues[910]. À titre illustratif,

---

[906] V. alinéa 2 de l'article 1er de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : « Les droits des personnes de décider et de contrôler les usages qui sont faits des données à caractère personnel les concernant (..) ». De cette énonciation, les auteurs du rapport Génération (*op. cit.*) ont déduit que ce texte consacre à la personne physique le droit de disposer de ses données et donc d'un *abusus* ; or ce texte n'affirme qu'un droit de contrôler l'usage qui peut être fait des données personnelles.

[907] L'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée « Charte») et l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne disposent que « toute personne a droit à la protection des données à caractère personnel la concernant ».

[908] V. préambule de la Déclaration des droits de l'homme et du citoyen (DDHC) de 1789 : « les droits naturels, inaliénables et sacrés de l'Homme », art. 2 DDHC : « Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression ».

[909] Il s'agit du principe l'extra-commercialité prévue par l'ancien article 1128 du code civil (« Les choses hors du commerce sont des choses qui ne peuvent être l'objet de convention » abrogée par l'Ord. no 2016-131 du 10 févr. 2016,), aujourd'hui la référence est celle de l'article 1162 du code civil lequel fait référence à l'ordre public : « Le contrat ne peut déroger à l'ordre public ni par ses stipulations, ni par son but, que ce dernier ait été connu ou non par toutes les parties ». Exemples de choses hors du commerce : les choses qui ont un caractère sacré ou intimement et nécessairement lié à la personne comme le corps humain, l'aspect moral des droits de la personnalité, les tombeaux et sépultures.

la Cour de cassation a prononcé la nullité absolue de la cession d'un fichier informatisé de clientèle non préalablement déclaré à la CNIL[911]. Cette jurisprudence vise uniquement la cession de fichiers de données personnelles entre organismes commerciaux. Avant le RGPD, ce type de cession était conditionné à la déclaration préalable à la CNIL. Cette formalité n'ayant pas été réalisée, la Cour de cassation a prononcé la sanction de la nullité absolue. Depuis l'entrée en vigueur du RGPD, il n'est pas interdit pour une société de céder à une autre société les données personnelles qu'elle détient de ses clients[912] ; en revanche, elle doit au préalable, d'une part, avoir informé le client de sa faculté de s'opposer à ce que ses coordonnées postales soient mises à disposition d'organismes extérieurs à des fins de prospection et d'autre part, avoir recueilli le consentement exprès si la cession concerne l'adresse électronique de la personne physique[913]. Si les organismes commerciaux peuvent céder entre eux des fichiers de données personnelles, il n'est pas permis à la personne physique de céder ses données personnelles. Le principe de l'inaliénabilité[914] des droits de la personnalité représente un obstacle à la reconnaissance au profit du titulaire de la donnée personnelle d'un « droit d'exploitation » sur celle-ci. Le titulaire des données à caractère personnel ne dispose pas, sur ses données, de la prérogative d'*abusus* qui est attribuée classiquement à un propriétaire[915]. En outre, il est relevé par la doctrine que la « conception personnaliste du droit des données personnelles (c'est-à-dire attachée à la personne) n'est pas très favorable aux propositions de patrimonialisation »[916]. Cette prise de

---

[910] Les données sont hors du commerce : V. article 1598 du code civil : « Tout ce qui est dans le commerce peut être vendu lorsque des lois particulières n'en ont pas prohibé l'aliénation ». V. également, l'article 16-5 du Code civil qui dispose que « les conventions ayant pour effet de conférer une valeur patrimoniale au corps humain, à ses éléments ou à ses produits sont nulles ».

[911] Cass. com. 25 juin 2013 n° 12-17.037 : La Cour de cassation a retenu l'illicéité du fichier en raison de l'absence de déclaration préalable auprès de la CNIL (obligation avant l'entrée en vigueur du RGPD). Ainsi, partant du principe que les choses illicites ne sont pas dans le commerce, l'objet de cette vente est illicite.

[912] CNIL, Cession ou échange de fichiers entre organismes commerciaux : est-ce légal ? : https://www.cnil.fr/fr/cnil-direct/question/cession-ou-echange-de-fichiers-entre-organismes-commerciaux-est-ce-legal.

[913] Art. L34-5 du code des postes et des communications électroniques.

[914] Répertoire de droit civil Inaliénabilité – Schütz R-N. – Juin 2014 (actualisation : Octobre 2020) « Selon le vocabulaire juridique Capitant, l'inaliénabilité est la « qualité (juridique) d'un bien (ou d'un droit) qui ne peut valablement être l'objet d'une aliénation, soit par l'effet d'une interdiction légale […], soit […] en vertu de la volonté de l'homme » (CORNU, Vocabulaire juridique, Assoc. Capitant, 2011, PUF). Le lexique des termes juridiques en donne une définition proche : « Caractéristique juridique d'un bien ou d'un droit qui ne peut pas faire l'objet d'une transmission d'une personne à une autre. L'inaliénabilité procède, généralement, d'une interdiction légale […]. Plus rarement, elle a sa source dans la volonté de l'homme, à travers une clause d'inaliénabilité […] » (GUINCHARD et DEBARD [dir.], Lexique des termes juridiques 2014-2015, 22e éd., Dalloz). Dans une première approche, nous retiendrons que l'inaliénabilité, dont la source est légale ou conventionnelle, est l'impossibilité de transférer, à titre gratuit ou à titre onéreux, une chose ou un droit ».

[915] V. *supra* n° 402 concernant la définition de l'*abusus*.

[916] La patrimonialisation fait, ici, référence, à la conceptualisation aux États-Unis de la marchandisation des données sur le marché. Aux Etats-Unis, absence d'un régime juridique général de la protection des données aux USA : Après le Pivacy Act de 1974, il a été adopté plusieurs lois sectorielles dans le privé pour la protection des données : HIPAA (Health Insurance Portability and Accountability Act) pour le respect de la vie privée des dossiers médicaux ; GLBA (Grammleach-Billey Act) pour les institutions financières ; Children's Online Privacy Protection Act limitant la collecte des données des enfants de moins de treize ans par des sites internet ; FCRA (Fair Credit Reporting Act) pour les profils de solvabilité des individus, ECPA (Electronic Communications Privacy Act) dans le secteur des télécommunications : Adrien Basdevant, Jean-Pierre Mignard, L'empire des données, essai sur la société, les algorithmes et la loi, Don Quichotte éditions, mars 2018, p.126.

position est confortée par le rapport du Sénat[917] qui écarte la possibilité d'accorder des droits de propriété aux personnes physiques en se fondant, d'une part, sur le rapport de force inégale entre les personnes physiques qui céderaient leurs données et les organismes commerciaux, qui les acquerraient, et d'autre part, sur le risque de marchandisation des attributs de la personnalité, tels que « la mise sur le marché des émanations de notre personne comme les éléments d'état civil : nom, domicile, date de naissance, nationalité »[918]. Il apparaît que ce principe d'inaliénabilité des données à caractère personnel est retranscrit en matière contractuelle. Ainsi, le principe de l'incessibilité des données est prévu par une clause spécifique dans le cadre d'un contrat de cloud computing. À titre d'exemple, il est mentionné dans certains contrats de cloud computing que « sauf obligation contraire imposée par la loi, vous acceptez que votre compte soit incessible et que tous les droits liés à votre identifiant Apple ou Contenu dans le cadre de votre Compte seront résiliés au moment de votre décès »[919]. Il s'agit d'une clause prévoyant l'inaliénabilité et l'intransmissibilité de certaines données à caractère personnel ayant fait l'objet du contrat cloud.

***414.*** Aujourd'hui, la donnée numérique demeure un « concept » juridiquement flou et mal appréhendé en raison de son caractère hétérogène alors même que la donnée est exploitée en masse et dont certaines organisations tirent des avantages économiques à les exploiter et à les revendre à d'autres acteurs[920]. Ce mouvement de la collecte « en masse » des données (« le big data »)[921] procurant des avantages financiers dans le marché actuel est à l'origine des atteintes au droit à la protection des données. C'est parce que la donnée dispose d'une valeur marchande au sein du marché que des acteurs ont mobilisé leurs forces et leurs savoir-faire technologiques pour les collecter, les traiter, les exploiter et les vendre sur le marché. En pratique, le marché économique des données est déjà constitué et des fichiers de données sont cédés par des courtiers de données sans que la question juridique du droit de propriété n'ait pas été tranchée.

---

[917] Rapport d'information n°441 (2008-2009) de Détraigne Y. et Escoffier A-M intitulé « la vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information ».

[918] Basdevant A. et Mignard JP., l'empire des données - essai sur la société, les algorithmes et la loi, Don Quichotte éditions, mars 2018, p.125.

[919] Contrat i.cloud d'Apple : https://www.apple.com/legal/privacy/fr-ca/.

[920] Illustration : Aujourd'hui, « la négociation de données personnelles se pratique actuellement à une autre échelle : et les vendent à des entreprises de tous secteurs qui souhaitent identifier des prospects intéressés par leurs produits. (…). 6 millions de foyers français figureraient ainsi dans la base d'Acxiom, l'un des neuf courtiers les plus puissants, qui généraient en 2012 un chiffre d'affaires total estimé à 426 millions d'euros, selon l'Université de Caroline du Nord » : Créquy P., Bientôt tous rentiers grâce à nos données personnelles ?, vie privée, 11 mai 2018 : https://www.mesdatasetmoi-observatoire.fr/article/bientot-tous-rentiers-grace-a-nos-donnees-personnelles.

[921] Bourgeois M., Droit de la donnée, principes théoriques et approche pratique, LexisNexis, 2017 : « L'irruption de l'informatique a marqué un tournant dans ces échanges car il en a permis l'amplification, que d'aucuns qualifient de révolution "Big data" et qui touche désormais tous les secteurs de notre société ».

Aux États-Unis, pour encadrer le marché des données, The California Consumer Privacy Act of 2018 (CCPA) donne aux consommateurs davantage de contrôle sur les informations personnelles que les entreprises collectent à leur sujet et garantit de nouveaux droits et en particulier le droit de refuser la vente de leurs informations personnelles. Au titre de cette loi, les entreprises sont tenues de fournir aux consommateurs certains avis expliquant leurs pratiques en matière de confidentialité. Le CCPA s'applique à de nombreuses entreprises, dont les courtiers en données[922].

***415.*** En définitive, il résulte qu'à ce jour aucun texte n'admet que la personne physique puisse revendiquer *un abusus* sur ses données à caractère personnel (au sens civil du terme pour caractériser la propriété) en raison du caractère inaliénable de ce droit fondamental. En conséquence, la personne physique, en fonction du droit civil français, ne remplit pas tous les attributs de la propriété et ne peut donc être considérée comme étant un propriétaire de ses données personnelles au sens juridique du terme. En revanche, dans la pratique des voix s'élèvent pour faire reconnaître le droit de propriété des personnes physiques sur leurs données. Ces propositions font l'objet d'une étude dans la partie suivante.

## B) L'attrait pour le droit de « propriété » comme moyen de protection des données à caractère personnel

***416.*** En France et à l'étranger, des voix s'élèvent pour demander la reconnaissance de la propriété privée des données personnelles et parfois même la rémunération. La propriété est perçue par certains auteurs comme un moyen de renforcer la protection des données des personnes physiques face aux entreprises d'internet. En renfort de ce plaidoyer pour la reconnaissance d'un droit de propriété, il est cité Proudhon qui « considérait la propriété comme « la plus grande force révolutionnaire qui existe », en ce qu'elle confère à l'individu la souveraineté sur son domaine propre »[923]. Il s'agirait ainsi d'acter la propriété de la personne physique sur ses données personnelles ou « une propriété de soi sur soi »[924].

***417.*** **Plan.** Il est envisagé d'étudier les arguments pour (1) et contre (2) la reconnaissance d'une propriété des données.

---

[922] Luciani A.-M., Les droits de la personnalité. Du droit interne au droit international, thèse, Paris I, 1996.

[923] Proudhon P-J., Théorie de la propriété (1862), L'Harmattan Éditeur, 1997.

[924] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Rapport (sous la direction de LÉGER L.), Mes data sont à moi - Pour une patrimonialité des données personnelles, janvier 2018 : https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf.

## 1) La volonté d'une reconnaissance d'un droit de propriété des données

Le plaidoyer pour la reconnaissance d'une propriété des données est fondé d'une part, sur des arguments tirés de l'évolution législative qui consacrent de nouveaux droits à la personne physique numérique ou l'*homo numericus*[925] (a) et d'autre part, sur la thèse de la patrimonialisation des données (b).

a) La revendication de la propriété des données par la constitution de nouveaux droits à *l'homo numéricus*

***418. La qualification du rapport juridique entre la personne physique et sa donnée par la propriété.*** La propriété des données est utilisée par certains auteurs pour décrire le rapport juridique existant entre la personne physique et ses données à caractère personnel. Plusieurs auteurs ont de manière récurrente revendiquer un droit de propriété sur les données personnelles[926]. Le Professeur Catala a écrit, concernant le droit à la propriété de l'information, « qu'on dénomme ou non "propriété" ce nouveau droit (...), peu importe au fond »[927]. Cela traduit l'existence d'un rapport juridique entre la personne physique et ses données qui nécessite d'être qualifié. En l'occurrence, on s'interroge sur l'application d'un droit de propriété des données. Le Professeur Catala, est l'un des premiers à avoir avancé la thèse « d'une propriété de l'information »[928] et le Professeur Vivant a considéré (concernant cette thèse) que « ce n'est pas l'aveu d'une légèreté dans la qualification, mais la marque du réalisme »[929]. Ainsi, la proposition d'un droit de propriété des données permettrait de retranscrire en termes juridiques le rapport existant entre la personne physique et ses données à caractère personnel.

***419.*** Il apparaît qu'en matière de cloud computing, des auteurs n'hésitent pas à utiliser le terme de « propriété » pour qualifier le rapport juridique entre la personne physique et sa donnée hébergée dans le cloud computing. Sur ce point, A. Chavernoz A. et C. Goupil affirment qu'« en pratique, il existe peu de débats entre les parties sur le fait que le contenu téléchargé par le client dans l'environnement cloud, ainsi que toute donnée qu'il crée via l'utilisation du service reste la propriété du client » [930]. Il y aurait, ainsi, une forme de consensus dans la pratique entre

[925] Expression de Mme le professeur Solange Ghernaouti, pour désigner « l'homme numérique ».

[926] Mallet-Poujol N., Appropriation de l'information : l'éternelle chimère : D. 1997, Chron. p. 330.

[927] Catala P., « La "propriété" de l'information », in Le droit à l'épreuve du numérique. Jus ex Machina, coll. "Droit, Éthique, Société », PUF , Paris, 1998, p.245-262.

[928] Ibid.

[929] Vivant M., La privatisation de l'information par la propriété intellectuelle, dans Revue internationale de droit économique 2006/4 (t. XX, 4), pages 361 à 388.

[930] Chavernoz A. et Goupil C., Contrats cloud : quels points d'attention dans la négociation ? La Semaine Juridique Edition Générale n° 23, 7 juin 2021, 627.

les professionnels dans les contrats de cloud computing pour désigner les données stockées comme étant la propriété de la personne physique. Certains prestataires de services mentionnent dans leurs conditions d'utilisation de services cloud que l'utilisateur demeure propriétaire de ses données. À titre d'exemple, il est précisé dans des conditions d'utilisation de Google que « vous restez propriétaire des données que vous nous confiez et nous pensons qu'il est important que vous puissiez y accéder »[931]. Dans le cadre d'un contrat de cloud computing, l'utilisateur, personne physique, serait « propriétaire » de ses données et le prestataire de services serait une sorte de « Garant » à qui les données ont été confiées. Il apparaît que la volonté au sein de la doctrine et de la pratique de faire reconnaître un droit de propriété des données numériques est récente et se pose depuis l'essor de la collecte « en masse » des données (« le big data)[932].

***420. La constitution d'une identité numérique.*** C'est à mesure que les législations reconnaissent des droits constitutifs d'une véritable « identité numérique » que l'individu est encouragé, aujourd'hui, à revendiquer un droit de propriété sur ses données à caractère personnel. Par exemple, il a été créé en 2011 « un délit d'usurpation d'identité numérique »[933] qui a été codifié à l'article 226-4-1 du Code pénal[934]. Ce délit sanctionne l'usurpation de l'identité et l'usage de données à caractère personnel troublant la tranquillité de la personne physique ou portant atteinte à son honneur ou à sa considération. La peine encourue est d'un an d'emprisonnement et de 15 000 euros d'amende. Sur ce fondement, la cour d'appel de Paris « a déclaré coupable du délit d'usurpation d'identité la personne qui utilise les coordonnées personnelles d'une autre pour créer de nouvelles adresses courriel et de nouveaux profils sur les réseaux sociaux dans le but de lui nuire »[935]. C'est, ainsi, dans un tel contexte d'évolution législative que « l'humain numérique » pourrait légitimement revendiquer un véritable droit de propriété sur ses données.

***421. La caractérisation du vol de données numériques.*** Depuis plusieurs années, le droit s'est emparé des problématiques de la protection des données à caractère personnel afin de conceptualiser des notions nouvelles et consacrer des droits aux individus. Ce mouvement de conceptualisation juridique a pris de l'essor et a connu ces dernières années une évolution

[931] Contrat cloud de Google : https://policies.google.com/terms.

[932] Grynbaum L., Le Goffic C., Morlet-Haïdara L., Droit des activités numériques, édition Dalloz, Collection Précis, 2e édition, 5/01/2022.

[933] La loi no 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2 ; JO 15 mars 2011). V. également, Quéméner M., La loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2) au regard des nouvelles technologies, Comm. Com. Électr., 2011, chron. 9.

[934] Article 226-4-1 du code pénal : « Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération .. ».

[935] CA Paris, 10 oct. 2014, n° 13/7387, Comm. Com. Élec. 2015, comm. 9, Caprioli E.

constante qui a été retranscrite non seulement dans les textes,[936] mais aussi dans les décisions de justice retenant la qualification de vol de données numériques[937]. À titre d'exemple, les juges du fond ont retenu la qualification de vol et d'abus de confiance le fait pour une salariée de transférer le jour de son départ de l'entreprise, des données informatiques confidentielles afin de les utiliser à des fins personnelles[938]. Puis, dans un arrêt inédit, la chambre criminelle de la Cour de cassation[939] confrontée à nouveau à la question de savoir si une donnée informatique peut faire l'objet d'un vol, précise davantage sa solution en considérant que « des données informatiques peuvent faire l'objet d'une « soustraction » indépendamment d'un quelconque support physique ». Tel qu'affirmé par Monsieur Auroy, il semblerait que la Cour de cassation s'oriente « vers une relative dématérialisation de l'élément matériel du vol, c'est-à-dire de l'acte de soustraction »[940]. La Cour considère de manière implicite que des données informatiques puissent s'analyser en une « chose », au sens de l'article 311-1 du Code pénal[941]. Alors même qu'en principe le terme de « chose » est juridiquement « appréhendé comme induisant une dimension matérielle »[942]. De prime abord, la position de la dématérialisation du vol semblerait, ainsi, être en opposition avec la définition classique de la « chose »[943]. En réalité, le législateur n'a jamais défini le terme « chose » malgré son emploi. En ce sens, cette jurisprudence peut être perçue comme permettant d'acter une évolution de ce qu'il faut entendre par la terminologie de « chose »[944]. Originellement, la notion de « soustraction », suppose en principe une interversion, même momentanée, de la possession, c'est-à-dire la perte matérielle de la chose[945]. C'est ainsi que la Cour de cassation dans l'arrêt *Baudet* définissait la notion de « *soustraction* » comme le fait de « prendre, enlever, ravir »[946]. Par la suite, la chambre criminelle a retenu une dématérialisation de la soustraction dès le début du XX$^{e}$ siècle, en admettant la qualification de « vol » en cas de soustractions dites « juridiques »[947]. Pour une soustraction « juridique »,

[936] Avec la consécration des droits de la personne concernée : v. chapitre 3 du RGPD ainsi que l'application des dispositions générales du Code pénal relatives aux délits de vol : v. C. pén., art. 311-1.

[937] CA Paris, pôle 4, ch. 10, 5 févr. 2014, nº 13/04833. V. aussi arrêt de la Chambre criminelle portant sur le vol et le recel de fichiers clients d'un ancien employeur : Cass. crim., 20 oct. 2010, no 09-88.387, Caprioli E., Comm. Com. Élec., 2011, comm. 30.

[938] TGI Clermont-Ferrand, ch. Corr., 26 sept. 2011 : illustration jurisprudentielle concernant le vol de données numériques. V. également, C. pén., art. 314-1.

[939] Cass. crim., 20 mai 2015, nº 14-81.336, inédit.

[940] Auroy B., Le vol de données informatiques ou l'avènement de la « soustraction 2.0 », Revue Lamy Droit de l'Immatériel, Nº 120, 16 novembre 2015.

[941] Ibid.

[942] Dreyer E., Droit pénal spécial, Ellipses, 2e éd., 2012, p. 398.

[943] Auroy B., Le vol de données informatiques ou l'avènement de la « soustraction 2.0 », Revue Lamy Droit de l'Immatériel, Nº 120, 16 novembre 2015.

[944] Ibid.

[945] Ibid.

[946] Cass. 18 novembre 1837, Bull. crim. 1837, nº 405.

[947] Cass. crim., 4 juin 1915, Bull. crim. nº 121 et Cass. crim., 14 mai 1958, Bull. crim. nº 391.

l'auteur ne s'empare pas de la chose dont il a la détention puisque celle-ci lui ayant été remise à titre précaire par la victime. Il est initialement un détenteur de la chose, puis ce dernier va venir « usurper la possession de celle-ci », ce dont il résultera une perte matérielle pour le propriétaire[948]. Dans cet arrêt du 20 mai 2015, nous ne sommes pas dans le cas d'une soustraction « juridique » puisque « l'auteur se contente d'en prendre connaissance et de les dupliquer. À aucun moment, il ne les détient ni ne les saisit directement. Parallèlement, le « propriétaire » conserve intégralement les données en cause, de sorte qu'il ne subit aucune perte de la chose, même temporaire »[949]. Dans ces conditions, il pourrait sembler difficile d'admettre une « soustraction de données »[950]. La Cour de cassation, pour légitimer la soustraction des données, avance deux théories. Pour la première, il s'agit d'admettre « qu'en s'emparant d'une information, l'auteur en soustrairait l'exclusivité »[951]. Pour la seconde, « c'est la valeur qui y est attachée qui serait soustraite »[952]. Ces deux théories ont pour effet d'appréhender pénalement le dommage que subit le titulaire des données personnelles. La Cour de cassation s'aligne sur ces théories en admettant la qualification de « vol » de données informatiques qui est caractérisé « dès lors que l'auteur a illégitimement en sa possession les données informatiques, peu important que leur propriétaire n'en est, à aucun moment, été dépossédé. Ce seul résultat d'une possession illégitime importerait davantage que l'acte de l'agent lui-même »[953]. Alors que la caractérisation du vol est conditionnée à la soustraction frauduleuse de la chose d'autrui, voici que les juges opèrent une extension de la caractérisation de vol aux données informatiques au profit du titulaire des données personnelles qu'elle qualifie de « propriétaire ». Il en résulte que la reconnaissance jurisprudentielle d'un vol de données numériques permet de conforter la thèse de la propriété des données et renforce par la même occasion les droits de *l'homo numericus*.

***422. Le droit de possession à travers l'exercice du droit à la portabilité des données.*** La reconnaissance de nouveaux droits, telle que « la portabilité des données »,[954] contribue, également, à rapprocher le cadre juridique de la donnée de celui applicable à la « propriété ». Le droit à la portabilité permet à la personne concernée de décider de récupérer ses données auprès d'un prestataire de services cloud pour les transférer auprès d'un autre prestataire de services.

[948] Cass. 18 novembre 1837, Bull. crim. 1837, nº 405.

[949] Ibid.

[950] Dreyer E., Droit pénal spécial, Ellipses, 2e éd., 2012, p. 398.

[951] Peltier V., Le secret des correspondances, PUAM, 1999, nº 757, p. 595.

[952] Ollard R., La protection pénale du patrimoine, Dalloz, Nouvelle bibliothèque des thèses, tome 98, 2010.

[953] Auroy B., Le vol de données informatiques ou l'avènement de la « soustraction 2.0 », Revue Lamy Droit de l'Immatériel, Nº 120, 16 novembre 2015.

[954] V. art. 20 du RGPD.

Dans ces conditions, la personne physique exerce sur ses données personnelles un droit de possession. La personne physique a la maîtrise sur ses données et par conséquent en a la possession puisqu' « il n'y a pas de maîtrise sans possession »[955]. C'est dans ce sens que ce droit à la portabilité se rapprocherait du droit de propriété. Ce rapprochement entre le droit à la portabilité et le droit de possession permet, ainsi, d'entériner l'application du principe civil suivant : « en fait de meubles, possession vaut titre »[956] ; et qui a pour effet d'admettre l'existence de la propriété au profit de la personne physique par le seul fait de la possession[957]. Si ce postulat est admis par certains, il n'emporte pas l'unanimité de tous[958].

b) La revendication de la propriété des données par la thèse de la patrimonialisation des données

***423. La revendication de la propriété et la rétribution au profit des personnes physiques pour l'exploitation des données personnelles.*** Certains auteurs ont constaté que dans l'ère de l'économie numérique, la revendication du droit de propriété sur les données personnelles apparaît « dès lors que l'information sur la personne fait non seulement l'objet d'un traitement massif, mais est devenue partie intégrante d'un marché, avec la gestion des « big data » et la négociation de données personnelles à des fins de profilage et de marketing »[959]. Pour la doctrine favorable à la reconnaissance d'un droit de propriété des données, dont Monsieur Destreguil, considère que « le droit de propriété gagnerait à être mieux défendu à l'avenir, car il paraît être une réponse naturelle à la question de l'identification du lien existant entre la personne et ses données et une solution utile aux nombreuses problématiques qu'elles suscitent »[960]. Concernant la détermination du droit de propriété, il a affirmé que « concrètement, la reconnaissance d'un droit de propriété pourrait se traduire ainsi : chacun des utilisateurs, en tant que propriétaire de ses données personnelles, pourrait les exploiter commercialement, en contrepartie d'un prix payé par les entreprises »[961]. Ce raisonnement s'inscrit dans la thèse de la patrimonialisation des données à caractère personnel et donc de l'application du concept de « propriété » aux données à caractère personnel.

[955] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Rapport (sous la direction de LÉGER L.), Mes data sont à moi - Pour une patrimonialité des données personnelles, janvier 2018 : https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf.

[956] Article 2276 du code civil.

[957] V. *supra* n° 402.

[958] V. *infra* n° 431 et suivants.

[959] Bernelin M., La patrimonialisation des données personnelles : entre représentation(s) et réalité(s) juridiques, JCP G 2019, Etude 1172.

[960] Destreguil M., Plaidoyer en faveur d'une approche propriétariste des données personnelles, RJPF 2019, nº 3.

[961] Ibid.

***424.*** La théorie de la propriété des données a été réactivée par le rapport de « Génération libre » intitulé « mes données sont à moi »[962]. Il est mis en avant que « de même que la révolution industrielle a rendu nécessaire le droit de propriété intellectuelle, la révolution numérique devrait créer un droit de propriété sur les données »[963]. Ce rapport propose, ainsi, d'instaurer une patrimonialité des données personnelles. Dans cette proposition, les personnes physiques seraient « des utilisateurs-producteurs » et plusieurs prérogatives leur seraient conférées, telles que : « la possibilité de contractualiser (éventuellement via des intermédiaires) l'usage de leurs données personnelles auprès des plateformes, afin de décider eux-mêmes de l'utilisation qu'ils souhaitent en faire ; la possibilité de monétiser (ou non) ces données en fonction des termes du contrat (vente, location...) préalablement conclu. La possibilité, à l'inverse, de payer le prix du service rendu par les plateformes sans leur céder nos données »[964]. Concernant cette dernière faculté, il s'agirait d'instaurer une forme d'un « prix de la privacy » en contrepartie d'un service fourni par ces plateformes, en l'occurrence, ici, de cloud computing. Cette proposition s'inspire de l'étude développée aux États-Unis par Monsieur Lanier[965] et des universitaires selon laquelle les personnes physiques devraient obtenir une rémunération des entreprises d'internet pour l'utilisation des données à caractère personnel[966].

***425.*** De manière plus approfondie, ce rapport propose de « rendre à l'individu producteur de données la propriété de ses données personnelles »[967]. À ce titre, il est mis en avant l'idée que « seul le droit de propriété permettra de garantir une maîtrise réelle de nos données. Seule la création d'un marché des data pourra rééquilibrer les rapports de pouvoir entre les plateformes et leurs utilisateurs, en dotant chacun d'entre nous d'un véritable capital »[968]. Le droit de propriété est mis, ici, en corrélation avec l'impératif de protection des données, laquelle serait possible en conférant à la personne physique des prérogatives lui permettant de disposer la maîtrise sur ses données à caractère personnel. En se fondant sur la conception large de la

---

[962] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Rapport (sous la direction de LÉGER L.), Mes data sont à moi - Pour une patrimonialité des données personnelles, janvier 2018 : https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf.

[963] Ibid.

[964] Ibid.

[965] Considéré comme étant le père de la réalité virtuelle, auteur de « Who owns The Future ? » (traduction en français - À qui appartient l'avenir ?) publié par Simon & Schuster en 2013.

[966] Lanier J., Arrieta Ibarra I., Goff L., Jimenez Hernandez D., Weyl E. G., « Should We Treat Data as Labor? Moving Beyond 'Free' » (traduction en français : " Devrions-nous traiter les données comme de la main-d'œuvre ? Au-delà de la "gratuité") Vol.1 N°1, Mai 2018 : copie électronique disponible sur https://ssrn.com/abstract=3093683.

[967] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Rapport (sous la direction de LÉGER L.), Mes data sont à moi - Pour une patrimonialité des données personnelles, janvier 2018 : https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf.

[968] Ibid.

propriété du Professeur Ginossar[969], qui englobe dans le patrimoine personnel les droits et obligations d'une personne juridique ce qui permet d'inclure, selon le rapport « les choses animées ou inanimées, mobilières ou immobilières, corporelles ou incorporelles, actuelles ou futures relevant d'une personne physique ou morale »[970] ; il s'agirait d'admettre que la personne physique à un patrimoine de données. Les données personnelles, selon ce rapport, peuvent s'envisager dans le contexte du droit des biens, comme des choses que l'on peut s'approprier[971] et contrôler. En ce sens, elles restent distinctes de la personne — de même que les « idées », qui elles aussi entretiennent un rapport intime avec l'individu qui les a produites, peuvent relever de la propriété intellectuelle »[972]. Il s'agirait d'appréhender les données comme objet « d'appropriation »[973] par le droit des biens et la propriété intellectuelle. À ce titre, il est défendu l'idée que « si la donnée personnelle peut être caractérisée dans le cadre du droit commun des biens, alors un droit de propriété peut émerger soit comme propriété intellectuelle, soit comme un contrat de licence »[974]. Il s'agirait de proposer un nouveau cadre juridique du marché de la donnée par « la mise en place d'un nouveau business model qui remet le citoyen au centre de l'exploitation de ses données »[975]. Pour prétendre à la propriété des données, il est affirmé « qu'il faut alors exercer une emprise possessoire sur la donnée personnelle, chose incorporelle »[976]. L'emprise possessoire est définie « comme le pouvoir de fait s'exerçant sur la donnée personnelle »[977]. Il est précisé que « la possession[978] est le constat juridique d'une situation de fait qui assure au possesseur une emprise sur l'objet de sa possession

[969] Ginossar S., Pour une meilleure définition du droit réel et du droit personnel, RTD civ. 1960, p37.

[970] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Rapport (sous la direction de LÉGER L.), Mes data sont à moi - Pour une patrimonialité des données personnelles, janvier 2018 : https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf.

[971] Il s'agit d'entreprendre une approche catégorielle de la réification des données : « La question de l'appropriation des données est le corollaire de l'enjeu économique que celles-ci représentent. La valeur de la donnée conduit à s'interroger sur sa réification. Toutes les données n'ont pas les mêmes caractéristiques et la même évolution de leur valeur dans le temps, ce qui influence leurs statuts juridiques » : Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.50, *op. cit.*.

[972] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Rapport (sous la direction de LÉGER L.), Mes data sont à moi - Pour une patrimonialité des données personnelles, janvier 2018 : https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf.

[973] « l'appropriation de la donnée s'effectue essentiellement par le biais de son traitement, qui débute dès la collecte, et par sa mise en valeur, notamment au travers de son tri au sein de bases de données et son analyse algorithmique » : Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.47, *op. cit.*.

[974] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.50, *op. cit.*.

[975] Ibid.

[976] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.57, *op. cit.*.

[977] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi – Pour une patrimonialité des données personnelles, p.58, *op. cit.*.

[978] L'article 2128 du Code civil définit la possession comme « la détention ou la jouissance d'une chose ou d'un droit ».

indépendamment de toute appropriation »[979]. Ainsi, la possession sur la donnée est appréhendée à travers la notion de « maîtrise » ou de « contrôle » sur les données. La caractérisation de la possession des données personnelles n'est possible que si deux éléments sont présents, à savoir : le corpus et l'animus. Le corpus de la possession correspond à l'accomplissement d'actes matériels par le possesseur sur la chose (exemple : des actes de détention au sens de l'article 2228 du code civil)[980]. L'animus correspond à la volonté du possesseur de conserver la chose[981]. Il en résulte que « le pouvoir factuel réside dans la capacité à la maintenir sous le sceau du secret ou d'en contrôler l'accès »[982]. Il faut, donc, comprendre par-là que le secret, le contrôle permet une emprise possessoire sur les données lesquelles sont volontairement maîtrisées par la personne physique. Il en résulte que le droit de propriété est conçu, ici, comme un outil de maîtrise sur les données. Ce rapport revendique l'idée lockéenne d'une « propriété de soi[983]» comme idéal de la modernité, affranchissant l'individu de l'emprise de toute transcendance »[984]. Par la maîtrise sur ses données, la personne physique est, donc, en mesure de les vendre, les louer, les céder voire de les gager[985]. À ce titre, il est proposé un « mécanisme de *fructus* de la donnée personnelle » permettant à la personne physique qui a consenti à l'exploitation de ses données d'être « en mesure d'en retirer les fruits (revenus) que d'autres font sur son dos »[986]. Les auteurs du rapport défendent l'idée que la personne physique « devrait recevoir une rétribution sur la masse de données brutes de la part de ceux qui vont produire la donnée agrégée »[987]. Cette proposition est partie du constat qu'« à l'heure actuelle, la donnée est

---

[979] Colin et Capitant, Cours élémentaire de droit civil français, 11ème éd. Dalloz 1947 par Julliot de La Morandière, t. 1, n° 1162 ; Terré F. et Simler Ph., Droit des biens, 9e éd. Dalloz 2014, n° 138 ; G. Cornu, vocabulaire juridique, 14e édition, Quadrige, la possession est le « pouvoir de fait exercé sur une chose avec l'intention de s'en affirmer le maître ». Cette définition implique donc l'existence d'une chose. Sur la reconnaissance d'un droit réel au possesseur : Chauveau, « Classification nouvelle des droits réels et personnels », rev. Crit. 1931.539, affirme que « le possesseur a pouvoir sur la chose comme le propriétaire... » ; in Landreau I., Peliks G., Binctin N., Pez-Pérard. v., rapport (sous la direction de Léger L.), Mes data sont à moi – Pour une patrimonialité des données personnelles, p. 58, *op. cit.*.

[980] Carbonnier, Droit civil – Les biens, 19ème éd. PUF 2000, n°119 p. 203.

[981] « Il ne peut y avoir de rapport possessoire sans volonté » : Jhering, Etudes complémentaires de l'esprit du droit romain – Du rôle de la volonté dans la possession, tome III, 2ème éd. A. Marescq aîné, Paris 1891, p. 17 et sq.

[982] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelle, p.60, *op. cit.*.

[983] Locke J., Second Treatise of Government, Chapter 5 : Property, 1690 : « Though men as a whole own the earth and all inferior creatures, every individual man has a property in his own person ; this is something that nobody else has any right to. » (traduction : Bien que les hommes dans leur ensemble possèdent la terre et toutes les créatures inférieures, chaque homme possède une propriété sur sa propre personne, sur laquelle personne d'autre n'a de droit.). Locke reprend en fait l'idée de « self- propriety » déjà développée par Richard Overton quelques années plus tôt : Landreau I., Peliks G., Binctin N., Pez-Pérard V., Rapport (sous la direction de LÉGER L.), Mes data sont à moi - Pour une patrimonialité des données personnelles, janvier 2018 : https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf.

[984] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelle, *op. cit.*.

[985] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelle, p.87, *op. cit.*.

[986] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.78, *op. cit.*.

[987] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.83 et 84, *op. cit.* : « des entreprises en France et à l'étranger commencent à créer des systèmes ad hoc pour permettre ce flux sur des transactions de données. Plusieurs expérimentations sont menées en Europe sur la monétisation des données personnelles, comme

monétisée, mais elle a fait l'objet d'une appropriation unilatérale, sans véritable circulation au profit du premier fournisseur de donnée : le citoyen ». Dans ce sens, la rétribution des données au profit de la personne physique permettrait de rétablir un équilibre dans le marché des données. Il s'agit de placer la personne physique au centre du business model de l'exploitation de la donnée, lequel se fonde, selon le rapport, « sur les droits de l'*homo numericus*[988] et la mise en place d'un nouveau modèle économique basé sur une réversion des revenus générés au citoyen, prix de son consentement sur une exploitation catégorielle ou selon la finalité poursuivie de ses données. »[989]. Cette proposition permet de passer d'un modèle gratuit (absence de rétribution des données au profit de la personne physique) à un modèle rétribué. Pour étayer ce raisonnement, le postulat est le suivant : « la donnée appartient à celui qui la fournit (conception classique) et le business model doit se fonder sur le premier fournisseur de donnée : le citoyen, qui sera rétribué sur la plus-value produite par la donnée, qu'elle soit première, générée ou agrégée »[990]. Cette proposition d'un nouveau business model d'exploitation des données intégrant la rétribution serait encadrée par le droit et par des mécanismes juridiques existants tels que le contrat de licence de marque, le droit de suite du droit d'auteur[991], ou encore une redevance par exploitation consentie (*pay per loyal use*, PPLU[992]) intégrée dans le système de collecte de données »[993]. Ces mécanismes juridiques proposés pour la mise en place d'une rétribution ont des avantages et des inconvénients et soulèvent la question de la faisabilité en termes juridique et technique.

***426.*** Concernant le contrat de licence de marque, la personne physique réaliserait un dépôt de son patrimoine de données à titre de marque. Les auteurs proposent la caractérisation du signe distinctif « par un nom, un pseudonyme, un chiffre (adresse IP, carte d'identité, carte vitale) » qui serait « enfermé dans un monopole de propriété ». Ce dépôt serait réalisé en utilisant la classe 45 de la classification de Nice qui comprend « les services de sécurité pour la protection des biens et des individus » ou aussi les « services de réseautage social en ligne ». Ce dépôt

---

MiData au Royaume-Uni ou MesInfos par la Fondation Internet Nouvelle Génération (Fing) en France. Aux USA, les databrokers existent déjà. Les courtiers de données, tels ACXIOM ou BLUEKAI génèrent des revenus sur les données personnelles qu'ils vendent aux entreprises. Acxiom aurait déjà recollecté 600 données par foyer sur 6 millions de foyers français ».

[988] Expression de Mme le professeur Solange Ghernaouti.

[989] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.87, *op. cit.*.

[990] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.87, *op. cit.*.

[991] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.90 et 91, *op. cit.*.

[992] Terminologie de GENERATION LIBRE.

[993] Landreau I., Peliks G., Binctin N., Pez-Pérard, v., p.89, Mes data sont à moi - Pour une patrimonialité des données personnelles, *op. cit.*.

permettra de réserver l'exploitation de cette marque qu'aux personnes titulaires d'un contrat de licence de marque et qui reversent au profit de la personne physique une redevance en fonction du volume et l'usage de la donnée. L'avantage de ce mécanisme est la création d'un monopole de propriété au profit de personnes physiques, les exploitants devront en amont toute exploitation passer par la personne physique. Les inconvénients peuvent résulter de la non-gratuité du dépôt, de la lourdeur du formalisme (nécessiter d'accomplir des formalités pour l'enregistrement du patrimoine de données) et la détermination du patrimoine des données. Autre inconvénient mis en lumière par les auteurs réside dans le fait que la donnée qui est exploitée par l'exploitant n'est pas la donnée statique ; « or la marque fige une partie de ses données à un moment précis »[994].

***427.*** S'agissant du droit de suite du droit d'auteur, il s'agirait d'intégrer la donnée « dans l'article L.111-1 du Code de propriété intellectuelle (CPI) en considérant que c'est une œuvre de l'esprit avec des attributs intellectuels et moraux et patrimoniaux. L'article L 111-2 du CPI permet que l'œuvre soit réputée créée indépendamment de toute divulgation, du seul fait de la réalisation, même inachevée de la conception de l'auteur. On permettrait, alors, au citoyen-internaute dont la donnée est absorbée par des mécanismes informatiques tels que les cookies ou autres, de considérer de facto que sa donnée issue de lui par ses activités sur Internet, est une œuvre de l'esprit, dont le contenu est exploitable sur d'autres supports »[995]. En raison de la distinctivité entre la propriété incorporelle et la propriété de l'objet matériel prévue à l'article L 111-3 du CPI, l'exploitation sur de nombreux supports serait, donc, possible. Pour cela, les auteurs du rapport indiquent qu'il suffirait « de rajouter dans l'article L 122-1 du CPI la mention : droit de collecte (de données) comme suit : « Le droit d'exploitation appartenant à l'auteur comprend le droit de représentation et le droit de reproduction et le droit de collecte numérique ». (..) Dès qu'une société exploite la donnée de l'internaute, elle devra verser un pourcentage ou une somme forfaitaire à l'internaute fabricant de la matière première »[996]. Il apparaît que cette proposition peut échouer face à l'exigence du caractère original. En effet, la controverse pourrait résider dans la difficulté d'identifier dans « des données de connexion ou aux données numériques telles le numéro de téléphone, la carte vitale, la carte bancaire », un caractère original[997].

---

[994] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.89, *op. cit.*.

[995] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.90 et 91, *op. cit.*.

[996] Ibid.

[997] Ibid.

***428.*** Quant à la redevance par exploitation consentie (*pay per loyal use*, PPLU), il s'agirait de permettre à la personne physique de devenir « créateur de base de données » dès lors qu'elle consent à l'exploitation de ses données. En admettant la qualité de « créateur de base de données », la personne physique est considérée comme étant « propriétaire de la donnée première et de la donnée générée ». Pour cela, les auteurs du rapport proposent « d'introduire un amendement à la définition du producteur de bases de données pour intégrer le créateur de base de données, le citoyen qui consent à ce que ses activités génèrent de la donnée exploitable »[998]. À ce jour, il existe deux conditions « pour être reconnu comme producteur de bases de données : personne physique ou société dont le siège social / administration centrale / établissement principal est en Europe et avoir réalisé l'investissement financier, humain, matériel substantiel (article L. 341-1 et L. 341-2 du Code de propriété intellectuelle) »[999]. En l'espèce, nous avons affaire à une personne physique résidante en Europe et dont l'investissement est, ici, « humain ». Si l'amendement est accueilli, on passerait, selon les auteurs, « du producteur de bases de données au créateur (citoyen) de base de données »[1000].

***429.*** S'agissant de la preuve de l'authenticité des données et l'identité de la personne physique, il est proposé plusieurs solutions techniques telles que l'adresse IP, la signature électronique, la chaîne des blocs[1001]. Concernant l'adresse IP, celle-ci ne permet pas d'authentifier une personne physique, mais un terminal. En revanche, la signature électronique, qui est basée sur des mécanismes cryptographiques, permet d'établir l'authentification forte d'une personne. Quant à la chaîne des blocs, elle permet de garantir l'authenticité des données, en revanche les blocs des chaînes actuelles ne permettent pas de stocker de larges volumes de données. À partir de la technologie des chaînes de blocs, les auteurs de ce rapport proposent de commercialiser les données en utilisant « le contrat autoexécutant pour établir les conditions de vente des données » ; il s'agit d'un contrat intelligent qui se fonde sur la technologie « des chaînes de blocs » laquelle est « infalsifiable et ineffaçable à partir du moment où les mineurs les ont validés, il est possible d'établir les conditions sous lesquelles les données peuvent être acquises

[998] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.94, *op. cit.*.

[999] Ibid.

[1000] Ibid.

[1001] Une chaîne de blocs est une « base de données distribuée, décentralisée de façon autonome ». La plus connue des chaînes de blocs est celle de Bitcoin, un protocole informatique qui permet notamment l'émergence d'applications distribuées se passant de tiers de confiance, telles que la cryptomonnaie. (…). Une chaîne de blocs peut être vue comme un grand registre ouvert à tous, dupliqué automatiquement et constamment sur beaucoup de serveurs, et dont les données numériques se situent dans des blocs infalsifiables. En effet, ces blocs sont chaînés ; chaque bloc est horodaté et dépend des précédents par des mécanismes cryptographiques. Une fois inclus dans la chaîne de blocs, un bloc ne peut être modifié car d'autres blocs s'ajoutent à la suite et si on modifie l'un d'eux, il faudrait aussi modifier tous les blocs qui précèdent. Des vérifications de l'intégrité des blocs de la chaîne de blocs s'opèrent, à chaque inclusion de nouveaux blocs, par de nombreuses personnes appelées les mineurs. Techniquement, toutes les duplications devraient être modifiées, car elles sont très sécurisées contre ce genre d'attaque ». : Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.113, *op. cit.*.

et comment doivent être effectués les paiements »[1002]. En revanche, cette technologie de la chaîne des blocs n'est qu'un registre des transactions et ne permet pas le stockage des données. Par ailleurs, si cette technologie permet d'apporter « la preuve de transfert et de cession d'une donnée personnelle d'un individu à une tierce partie », cette solution « technico-juridique » comporte certaines limites liées à la non-territorialité des données[1003], l'identité numérique et l'identité physique[1004].

***430.*** Concernant la non-territorialité des données, la difficulté réside dans la nature même d'une donnée « qui peut être aisément copiée » et cela rend « complexe le maintien de droits de propriété exclusifs et non rivaux ». Tout d'abord, « les données peuvent être facilement copiées et stockées sans le consentement de la contrepartie. Ensuite, « que le droit a des limites territoriales », puisque « si une personne mal intentionnée décide de piller des données personnelles et se trouve géographiquement à un endroit où la règle de droit est différente, il sera très difficile de la faire respecter »[1005].

***431.*** S'agissant de l'identité numérique et l'identité physique, elle est mise en difficulté dans la technologie des chaînes de blocs puisque « le système de transaction est par construction entièrement pseudonyme ». Il en résulte, tout d'abord, « qu'il est difficile de vérifier que la clé privée n'a pas été subtilisée et que la transaction est bien légitime » ; ensuite que « même s'il n'y a pas eu de vol de cette clé privée, rien ne garantit que la personne physique dispose de ses droits et est en capacité (absence de tutelle par exemple)[1006]. Les auteurs du rapport considèrent « que ces difficultés liées à l'identité sont réelles et ont un impact potentiel en termes juridiques. Cela renvoie directement à un problème de répudiation du contrat, où le co-contractant mécontent aura un plus grand intérêt à ne pas honorer ses engagements »[1007]. Pour remédier à ces difficultés, il est proposé le recours à « la multi-signature »,[1008] mais cette solution risque d'alourdir le processus de formalisation de la transaction.

---

[1002] Illustration : « Dans le cas d'Ethereum, les paiements se font en ethers. L'ether est l'unité d'une des nombreuses cryptomonnaies que l'on trouve dans les chaînes de blocs. Les possesseurs d'ethers peuvent ensuite convertir cette cryptomonnaie en euros ou dans autre monnaie fiduciaire via une plateforme d'échange. Dans la chaîne de blocs Ethereum, les contrats intelligents sont écrits dans un langage informatique dit Solidity, qu'il faut évidemment maîtriser. Il est aussi indispensable de prévoir tous les cas d'application des contrats car ici, code is law.» : Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.115, *op. cit.*.

[1003] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.122, *op. cit.*.

[1004] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.124, *op. cit.*.

[1005] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.122, *op. cit.*.

[1006] Ibid.

[1007] Ibid.

[1008] Ibid.

***432.*** Pour parachever cette proposition, il est avancé l'idée de mettre en place « un marché des droits relatifs à l'utilisation des données. Une sorte de marché de la diffusion hertzienne appliquée à l'utilisation des données personnelles »[1009]. Dans ce sens, la chaîne de blocs serait conçue comme « un registre de référence enregistrant non pas les transactions des données elles-mêmes, mais les octrois de droit d'utilisation de ces données personnelles »[1010]. Par ce mécanisme, « les transactions enregistrées dans la chaîne de blocs pourraient constituer la preuve d'octroi d'usage des données et de ses modalités d'utilisation. Cela pourrait constituer une preuve légale de l'utilisation de données personnelles ». Il en résulterait que c'est « cet élément de preuve d'octroi de droit, qui est susceptible de prendre de la valeur et donc de prendre la forme d'un actif échangé, plutôt que les données elles-mêmes »[1011]. En définitive, ces auteurs affirment que l'enjeu résiderait, ici, dans « la construction d'un marché de droits d'utilisation des données préalable à toute tentative de création de marché de la donnée »[1012].

***433.*** Bien que l'objectif de la thèse de patrimonialisation des données soit légitime, en ce qu'il vise un rééquilibrage des pouvoirs dans le marché de la data entre les personnes physiques et les exploitants des données, il apparaît que celle-ci n'est pas compatible avec les caractéristiques juridiques du droit de la propriété et plus généralement avec l'état du droit positif français et européen. En effet, pour certains auteurs « la mise en œuvre d'une « propriété sur les données » semble délicate »[1013]. En outre, les propositions découlant de cette thèse semblent ne pas pouvoir être réalisées compte tenu des difficultés techniques pour la gestion contractuelle[1014], la commercialisation des données[1015] et le contexte international d'une libre circulation des données[1016]. En réponse à cette thèse, des auteurs vont s'opposer à l'idée d'une reconnaissance d'une propriété, dont les raisons sont étudiées dans la partie suivante.

---

[1009] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Mes data sont à moi - Pour une patrimonialité des données personnelles, p.125, *op. cit.*.

[1010] Ibid.

[1011] Ibid.

[1012] Ibid.

[1013] Mattatia F., Yaïche M., « Être propriétaire de ses données personnelles : peut-on envisager un régime spécifique ? (partie II) », RLDI 2015/6, p. 41, spéc. II, dans Netter E., Ndior V., Puyraimond J-F, Vergnolle S. Regards sur le nouveau droit des données personnelles. Centre de droit privé et de sciences criminelles d'Amiens. 2019, 979-10-97323-05-9. hal-02357967.

[1014] V. *supra* n° 421, concernant la proposition d'un contrat de licence de marque.

[1015] V. *supra* n° 424, concernant l'utilisation de la technologie de la blockchain (blocs de chaines) pour la commercialisation.

[1016] Le cadre légal français et européen France est favorable à la libre circulation des données, v. *supra* n° 105.

## 2) Le rejet de la proposition d'une propriété des données

***434.*** La reconnaissance d'un droit de propriété des données est soutenue par la doctrine favorable à la thèse de la patrimonialisation, mais celle-ci n'est pas partagée par l'ensemble de la doctrine. Il est question, dans cette partie, d'étudier l'argumentaire des opposants à la thèse de la patrimonialisation des données.

***435. Plan.*** Il apparaît que la thèse de la patrimonialisation des données est rejetée par les partisans de la théorie « personnaliste » (a) en se fondant sur des arguments tirés des exigences légales du droit français et européen tels que l'absence d'un droit réel (b), le caractère inaliénable du droit à la protection des données(c), l'absence d'un effet translatif de propriété dans les contrats de cloud computing (d), l'absence d'une dimension purement exclusive dans le rapport à la possession (e) et l'absence de « valeur » d'une donnée personnelle isolée (f).

a) La pertinence de la théorie personnaliste face à la thèse de la patrimonialisation des données

***436.*** En doctrine, la question d'un droit de propriété des données a suscité un vif débat[1017]. Les opposants à la thèse de la patrimonialisation des données s'inscrivent dans une logique dite « personnaliste », c'est-à-dire qui se fonde sur les droits fondamentaux de la personne physique. Cette théorie accorde des droits à la personne physique et des obligations au responsable du traitement des données. À ce jour, la France et l'Union européenne appliquent cette théorie pour établir le cadre légal de la protection des données à caractère personnel. C'est à travers le prisme de cette théorie qu'est envisagée l'analyse des critiques de la théorie de la patrimonialisation des données personnelles.

***437.*** Le professeur Vivant a indiqué concernant la propriété de l'information « mais si, ainsi que nous l'avons fait, on peut à cet égard évoquer une « réservation » de l'information comme se plaît à le faire ce qu'on a parfois baptisé du nom d'« École de Montpellier », il serait impropre de parler de propriété »[1018]. Concernant la thèse de la patrimonialisation des données, la CNIL a considéré que « cette approche rompt avec nos convictions humanistes et personnalistes profondes, dans lesquelles le droit de la protection est un droit fondamental, faisant écho à l'essence même de la dignité humaine : naturellement, ce droit n'est pas un droit marchand »[1019]. Le Conseil national du numérique estime également que « l'introduction d'un système

[1017] Benabou V.-L., Rochfeld J., A qui profite le clic ? Odile Jacob, 2015. Purtova N., Property Rights in Personal Data. A European Perspective, Kluwer Law International 2012. Hoeren T., Big Data and the Ownership in Data: Recent Developments in Europe, European Intellectual Property Review 2014, p. 751.

[1018] Vivant M., La privatisation de l'information par la propriété intellectuelle, dans Revue internationale de droit économique 2006/4 (t. XX, 4), pages 361 à 388.

[1019] Fagot V., Et si chacun vendait ses données personnelles sur Internet ? Le Monde, 26 janvier 2018.

patrimonial pour les données à caractère personnel est une proposition dangereuse »,[1020] car « elle repose sur la négation du rapport de force existant avec les entreprises, alors même qu'elle ne pourrait générer que des revenus très faibles aux personnes et déboucherait sur un renforcement des inégalités entre citoyens quant à leur capacité de gérer, protéger et monétiser leurs données, fonctions qui seraient alors exercées par le marché´ »[1021].

***438.*** Il s'agit, ici, de remettre en cause la théorie de la propriété et donc de la thèse de la patrimonialisation des données, à travers les exigences du droit français et européen. Il apparaît que le principal argument des opposants à la reconnaissance d'un droit de propriété des données à caractère personnel[1022] est fondé « tant sur l'impossibilité théorique que l'impossibilité pratique d'un droit réel sur ces données »[1023].

b) L'absence d'un droit réel

***439.*** Tel qu'il a été étudié dans nos développements précédents, il ne fait pas de doute que la personne physique n'a pas la capacité d'exercer un droit réel sur ses données[1024]. Monsieur Destreguil affirme, à ce sujet, que le concept de propriété ne peut s'appliquer à la personne physique sur données dans la mesure qu'elle n'exerce concrètement aucun droit réel sur ses données. C'est, donc, en raison de l'incorporalité de la donnée que la personne physique est dans l'impossibilité d'exercer un pouvoir direct et immédiat sur ses données. De ce raisonnement, il en découle que le défaut d'un droit réel justifierait l'exclusion de la qualification d'une propriété des données personnelles. Sur ce point, d'autres auteurs considèrent que si les personnes physiques ne disposent pas d'un droit réel sur leurs données personnelles, elles exercent du moins un droit personnel sur l'usage de la chose permettant d'établir la propriété[1025]. Alors que d'autres auteurs refusent de reconnaître une propriété des données à la personne physique mais accordent « le droit de décider des usages qui en sont

[1020] Conseil national du numérique, La neutralité des plateformes, Rapport 2014 ; Créquy P., Bientôt tous rentiers grâce à nos données personnelles ? vie privée, 11 mai 2018 : https://www.mesdatasetmoi-observatoire.fr/article/bientot-tous-rentiers-grace-a-nos-donnees-personnelles.

[1021] Netter E., Ndior V., Puyraimond J-F, Vergnolle S. Regards sur le nouveau droit des données personnelles. Centre de droit privé et de sciences criminelles d'Amiens. 2019, 979-10-97323-05-9. hal-02357967.

[1022] Pour un plaidoyer contre la reconnaissance de la « propriété » des données par les géants de l'internet : Behar-Touchais M., L'effectivité du droit face à la puissance des géants de l'Internet, IRJS-éditions, 2015, p. 73. V. également, N. Ochoa, Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition, RFDA 2015. 1157.

[1023] Destreguil M., Plaidoyer en faveur d'une approche propriétariste des données personnelles, RJPF 2019, nº 3.

[1024] V. *supra* n° 404.

[1025] Ibid.

faits » lequel serait un attribut de la personnalité[1026]. En rattachant, le droit de décider des usages sur les données à un attribut de la personnalité, c'est rejeter formellement la théorie de la patrimonialisation des données et afficher de manière univoque l'attachement à la thèse personnaliste des données personnelles.

***440.*** Outre l'absence d'un droit réel, les partisans de la théorie « personnaliste » vont avancer d'autres arguments convaincants, tels que le caractère inaliénable du droit à la protection des données.

c) Le caractère inaliénable du droit à la protection des données

***441.*** Quant à l'impossibilité théorique de caractériser une propriété des données, plusieurs auteurs vont émettre des critiques à l'égard de la thèse de la patrimonialisation des données en se fondant sur les principes directeurs du droit français et européen. Pour ces auteurs, le fait de conférer un droit de propriété sur les données soulève des difficultés juridiques ; cela reviendrait à dire que « la protection des données n'est plus un droit fondamental ni un droit de la personnalité »[1027]. Pour contrer la thèse de la patrimonialisation des données, il est avancé l'argument juridique qu'« un droit de propriété implique un droit d'être dépossédé, alors qu'un droit de la personnalité est inaliénable »[1028]. La réticence doctrinale d'une reconnaissance d'un droit de propriété des données est légitimée au regard du caractère inaliénable du droit fondamental à la protection des données à caractère personnel[1029]. En effet, la protection des données à caractère personnel est un droit fondamental attaché à la personne et comme tous les droits de la personnalité, ils sont inaliénables[1030]. Pour rappel, un droit inaliénable est un droit inhérent à un individu du seul fait de ce qu'il est (condition humaine), il ne peut être ni transmis, ni cédé, ni vendu et s'éteint au décès de la personne qui le détient[1031]. En application du caractère inaliénable du droit à la protection des données personnelles, celles-ci sont considérées comme étant des « biens immatériels » hors du commerce, elles ne peuvent pas être vendues. La personne physique n'est, donc, pas en mesure de céder à titre onéreux ou à titre gratuit ses

[1026] Cousin A, « La Data au cœur du projet de loi pour une République numérique », D. 2018, p. 2176, dans Netter E., Ndior V., Puyraimond J-F, Vergnolle S. Regards sur le nouveau droit des données personnelles. Centre de droit privé et de sciences criminelles d'Amiens. 2019, 979-10-97323-05-9. hal-02357967.

[1027] CNIL, Cahier IP n°1, vie privée à l'horizon 2020, p.55, *op. cit.*.

[1028] Ibid.

[1029] V. *supra* n° 408 (droit inaliénable).

[1030] Étude annuelle 2014, Conseil d'Etat, le numérique et les droits fondamentaux, 8 septembre 2014 : https://www.conseil-etat.fr/publications-colloques/etudes/le-numerique-et-les-droits-fondamentaux.

[1031] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Rapport (sous la direction de Léger L.), Mes data sont à moi - Pour une patrimonialité des données personnelles, p.17, janvier 2018 : https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf.

données à caractère personnel. À ce titre, le Conseil d'État, dans son étude annuelle sur le numérique et les droits fondamentaux[1032], a affirmé que « les données personnelles ne pourraient pas être monétisées au nom de la protection des libertés fondamentales : la personne étant réputée indisponible et ne pouvant faire l'objet d'un commerce, les data qui en émanent devraient elles aussi être exclues du marché »[1033].

***442.*** En outre, il apparaît que le principe d'inaliénabilité des données à caractère personnel est retranscrit dans les contrats de cloud computing[1034]. En revanche, cette interdiction de principe connaît une limite à l'égard des organismes commerciaux qui céderaient entre eux des fichiers de données personnelles. Tel qu'étudié ci-dessus[1035], il n'est pas interdit pour une société de céder à une autre société les données personnelles qu'elle détient de ses clients dès lors que certaines conditions sont remplies[1036]. Ce tempérament ne s'applique qu'aux organismes commerciaux, la personne physique ne peut pas quant à elle céder ses données personnelles en application du principe de l'inaliénabilité[1037]. Il en résulte que cette conception personnaliste du droit des données personnelles s'oppose aux propositions de patrimonialisation des données, c'est-à-dire à la marchandisation des données[1038]. Cette opposition à la thèse de la patrimonialisation des données est justifiée par le refus d'une marchandisation des attributs de la personnalité, tels que les éléments d'état civil : nom, domicile, date de naissance, nationalité[1039]. Il est rappelé que « le rapport de droit de l'individu sur ses informations est un droit de la personnalité » et que « le lien entre la personne et ses données nominatives est forgé autour de sa dignité et induit des prérogatives spécifiques »[1040].

---

[1032] Étude annuelle 2014, Conseil d'Etat, le numérique et les droits fondamentaux, 8 septembre 2014 : https://www.conseil-etat.fr/publications-colloques/etudes/le-numerique-et-les-droits-fondamentaux.

[1033] Landreau I., Peliks G., Binctin N., Pez-Pérard V., Rapport (sous la direction de Léger L.), Mes data sont à moi - Pour une patrimonialité des données personnelles, p.17, *op. cit.*.

[1034] V. *supra* n° 408 (droit inaliénable).

[1035] V. *supra* n° 408 (cession de fichiers de données à caractère personnel).

[1036] CNIL, Cession ou échange de fichiers entre organismes commerciaux : est-ce légal ? : https://www.cnil.fr/fr/cnil-direct/question/cession-ou-echange-de-fichiers-entre-organismes-commerciaux-est-ce-legal.

[1037] V. *supra* n° 408 (droit inaliénable).

[1038] La patrimonialisation fait, ici, référence, à la conceptualisation aux États-Unis de la marchandisation des données sur le marché. Aux Etats-Unis, absence d'un régime juridique général de la protection des données aux USA : Après le Pivacy Act de 1974, il a été adopté plusieurs lois sectorielles dans le privé pour la protection des données : HIPAA (Health Insurance Portability and Accountability Act) pour le respect de la vie privée des dossiers médicaux ; GLBA (Grammleach-Billey Act) pour les institutions financières ; Children's Online Privacy Protection Act limitant la collecte des données des enfants de moins de treize ans par des sites internet ; FCRA (Fair Credit Reporting Act) pour les profils de solvabilité des individus, ECPA (Electronic Communications Privacy Act) dans le secteur des télécommunications : Adrien Basdevant, Jean-Pierre Mignard, L'empire des données, essai sur la société, les algorithmes et la loi, Don Quichotte éditions, mars 2018, p.126.

[1039] Rapport d'information n°441 (2008-2009), p.125, de Détraigne Y. et Escoffier A-M intitulé « la vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information ».

[1040] Warusfel B., Mallet-Poujol N., Costes L. (sous la direction de Vivant M.), Le Lamy droit du numérique, Partie 1 Numérique et biens, Division 2 Bases de données et autres ensembles informationnels, Chapitre 2 Protection des bases de données et autres ensembles informationnels, 205 - Des données aux ensembles de données, édition lamy expert, Wolterz Kluwer, mis à jour 04/2022.

***443.*** En sus, la doctrine considère que « l'octroi d'un droit de propriété exclusif sur une donnée personnelle aboutirait à des situations absurdes. À titre illustratif, la première personne qui "dépose" ou utilise pour la première fois un "prénom" pourrait par exemple se prévaloir d'une originalité sur celui-ci empêchant toute autre personne de l'employer au motif qu'elle serait le contrefacteur »[1041]. Pour appuyer cette prise de position, il est mis en avant qu'en cas de vente d'une donnée personnelle, il serait difficile de concevoir qu'un individu cède également tous les attributs et prérogatives attachés à celle-ci. Prenons l'exemple d'une personne qui vendrait son nom patronymique ; cet individu devrait disposer d'un droit inaliénable de pouvoir utiliser son nom à des fins d'identification (pour recevoir des courriers) ou encore d'interactions sociales. On voit mal comment le lui refuser »[1042]. Cet argument logique, du point de vue des effets juridiques, remet en cause la thèse d'une rétribution financière pour l'exploitation des données personnelles telle que défendue par Génération libre[1043].

d) L'absence d'un effet translatif de propriété dans les contrats de cloud computing.

***444. L'absence d'un effet translatif de propriété dans les contrats de cloud computing.*** En outre, il apparaît que dans le cadre de la contractualisation des prestations de services cloud, des auteurs ont considéré que l'exploitation commerciale des données à caractère personnel « conduit certains à préconiser une appropriation de l'information personnelle, aux fins d'assurer un droit de contrôle de la diffusion commerciale de ses données »[1044]. Ce raisonnement a pu être critiqué et considéré comme étant dangereux en raison que cette démarche hypothèque le principe de dignité de la personne[1045]. En effet, des auteurs ont considéré que cette démarche « instaure une faculté pour l'individu de disposer de l'information le concernant quand seule la jouissance de cette information est véritablement en jeu »[1046]. Ce raisonnement permet de mettre en lumière que la personne physique lorsqu'elle accepte que le prestataire de services cloud puisse utiliser et exploiter les données à caractère, elle ne transfère pas l'*abusus* (c'est-à-dire la faculté de disposer de la chose), mais uniquement la jouissance de la donnée ou comme certains le mentionne l'usage de la donnée personnelle. Il en résulte que si

[1041] Basdevant A., Mignard J-P., L'empire des données, essai sur la société, les algorithmes et la loi, Don Quichotte éditions, mars 2018, p.120.

[1042] Basdevant A. et Mignard JP., l'empire des données - essai sur la société, les algorithmes et la loi, p.127, *op. cit.*.

[1043] V. *supra* n° 418 (rétribution financière).

[1044] Warusfel B., Mallet-Poujol N., Costes L. (sous la direction de Vivant M.), Le Lamy droit du numérique, Partie 1 Numérique et biens, Division 2 Bases de données et autres ensembles informationnels, Chapitre 2 Protection des bases de données et autres ensembles informationnels, 205 - Des données aux ensembles de données, édition lamy expert, Wolterz Kluwer, mis à jour 04/2022.

[1045] Ibid.

[1046] Ibid.

la personne physique n'est pas en mesure de céder ses données, elle ne peut en conséquence prétendre être propriétaire des données en raison du défaut de l'attribut de l'*abusus*.

***445.*** Le contrat cloud peut prévoir des clauses dans lesquelles l'utilisateur concède au fournisseur une licence pour collecter[1047], traiter les données[1048] et les communiquer à des tiers. À partir de cette autorisation « débute une longue chaîne de transmission, partage, vente de fichiers sur laquelle l'individu n'a plus le contrôle, ni formel ni encore moins effectif »[1049]. Dans le cadre de cette licence, il est intéressant de cerner la conception qu'ont les prestataires de services cloud concernant leurs prérogatives de traitement des données des clients. Il est mentionné dans des contrats cloud, que l'utilisateur serait « propriétaire » de ses données et le prestataire serait une sorte de « Garant » à qui les données ont été confiées[1050]. Cette conception semble faussée puisque la propriété appréhendée, dans sa conception classique, ne peut s'appliquer à la donnée en raison du caractère inaliénable du droit fondamental à la protection des données[1051]. Si l'on admet, également, un droit de propriété, on admet par la même occasion la possibilité d'une dépossession ; permettre une dépossession susciterait des interrogations au regard de la protection conférée par sa valeur de droit fondamental[1052]. Par ailleurs, le fait de confier des données implique la restitution à l'identique sans altération alors qu'ici le fournisseur de services cloud va exploiter les données et donc porter atteinte à l'intégrité des données. En effet, même si les données sont restituées à son « propriétaire », il n'en demeure pas moins que d'autres copies peuvent exister dans d'autres serveurs, lesquelles continueront à être utilisées par le prestataire de services cloud lui-même ou d'autres organisations. Également, certains auteurs retiennent que « la patrimonialisation des données pourrait n'apporter aucun bénéfice pour les personnes et plutôt « conduire à l'inscription de clauses de cession obligatoire dans les

---

[1047] Illustration, dans le contrat i.cloud d'Apple : S'agissant de la collecte et utilisation des données à caractère non personnels, c'est-à-dire les informations qui ne permettent pas d'identifier une personne physique, Apple indique pouvoir recueillir, utiliser, transférer et divulguer ces renseignements à n'importe quelle fin ; tels que la profession, la langue, le code postal, l'indicatif régional et l'identifiant unique d'appareil, l'URL de renvoi ainsi que l'endroit et le fuseau horaire où un produit Apple est utilisé, les activités des clients sur nos sites Web, les services iCloud (…), les termes de recherche de l'utilisateur. Cette liberté prise par Apple s'explique par le fait que les données ainsi concernées ne sont pas en mesure de porter atteinte à des personnes déterminées : https ://www.apple.com/legal/privacy/fr-ca/.

[1048] Illustration, dans le contrat i.cloud d'Apple : Concernant l'utilisation des informations à caractère personnel, Apple, énonce dans sa politique de confidentialité, qu'elle est susceptible, avec la permission de l'utilisateur, de traiter les données à caractère personnel dans des cas précis ; tels que le respect d'une obligation juridique, l'exécution d'un contrat auquel est parti l'utilisateur, protéger les intérêts légitimes d'Apple, pour créer, développer les produits, services, à des fins de sécurité de compte et de réseau, vérifier l'identité de l'utilisateur, pour envoyer des avis importants, pour administrer ces programmes. Ainsi si Apple est susceptible de traiter les données stockées dans icloud, alors elle est tenue au respect des règles édictées par le RGPD et se mettre en conformité avec ces obligations : https ://www.apple.com/legal/privacy/fr-ca/.

[1049] Basdevant A. et Mignard JP., l'empire des données – essai sur la société, les algorithmes et la loi, p.118, *op. cit*..

[1050] Sur ce point, il est précisé dans des conditions d'utilisation de Google « vous restez propriétaire des données que vous nous confiez et nous pensons qu'il est important que vous puissiez y accéder » https://policies.google.com/terms.

[1051] V. supra n° 408.

[1052] Ibid.

contrats entre opérateurs et, par voie de conséquence, à un plus grand risque de dépossession »[1053].

***446.*** Pour conforter la thèse de l'inadaptation du concept de « propriété » appliquée à la protection des données à caractère personnel, certains auteurs en doctrine se fondent sur l'idée qu'« aucune des obligations contractuelles contenues dans un contrat infonuagique ne saurait s'analyser en un transfert de propriété, que celle-ci soit corporelle ou incorporelle »[1054]. Il s'ensuit que c'est en raison de l'absence d'un effet translatif de propriété sur les données que la conception classique du droit de propriété ne peut être retenue au sein des contrats de cloud computing.

e) L'absence d'une dimension purement exclusive dans le rapport à la possession

***447.*** Dans sa conception classique, la propriété comprend une dimension purement exclusive dans le rapport à la possession alors que le rapport des personnes à « la donnée » n'est pas caractérisé par une dimension exclusive. En effet, cette dimension exclusive dans le rapport à la possession semble absente puisque c'est au contraire « la circulation et l'usage attendu qui vont créer de la valeur »[1055]. Dans une approche classique du droit de propriété, il y a l'idée d'une éventuelle appropriation définitive ; alors que dans le cadre de la donnée, il est possible de reconnaître des droits personnels concurrents sans pour autant que cela vienne priver la possession ou l'usage de la donnée[1056]. La propriété a, ainsi, une approche exclusive dans la possession ; alors que dans le cadre de la donnée ce qui va lui conférer de la valeur, c'est au contraire la circulation. Il apparaît que l'AGD[1057] a pris en compte cette distinction et a choisi de quitter « le modèle de la propriété construite autour des choses tangibles ou sa transposition aux titres immatériels »[1058]. Ce texte inaugure une nouvelle forme de circulation économique, qui s'articule autour « de l'organisation de l'accès et des modalités de partage des objets numériques liées aux capacités de réplication propres à cet univers » et ce pour envisager « des

[1053] Avis sur la libre circulation des données en Europe, 28 avr. 2017, p. 4, dans Netter E., Ndior V., Puyraimond J-F, Vergnolle S. Regards sur le nouveau droit des données personnelles. Centre de droit privé et de sciences criminelles d'Amiens. 2019, 979-10-97323-05-9. hal-02357967.

[1054] Bourgeois M., JurisClasseur Communication, Fasc. 962 : cloud computing – Les défis contractuels du Cloud Computing, 1er mai 2020.

[1055] Basdevant A. et Mignard JP., l'empire des données - essai sur la société, les algorithmes et la loi, p.113, *op. cit*..

[1056] Ibid.

[1057] Proposition de Règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (Acte sur la gouvernance des données), 2020/0340 (COD), le 25 novembre 2020 : https://ec.europa.eu/transparency/regdoc/rep/1/2020/FR/COM-2020-767-F1-FR-MAIN-PART-1.PDF.

[1058] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279. V. également, Benabou V.L, Rochfeld J., *A qui profite le clic ?* Odile Jacob, 2015.

modes d'échanges fondés sur la multiplication et non sur l'exclusivité »[1059]. S'agissant de cette trajectoire européenne affirmée, la doctrine félicite les autorités européennes « de l'abandon de certaines chimères, telles que la propriété des données »[1060]. Cette différence fondamentale, entre une approche fondée sur l'exclusivité pour la propriété et sur la circulation pour les données, permet de conforter la thèse que le concept de « la propriété » ne soit pas adapté pour renforcer la protection des données à caractère personnel dans les contrats de cloud computing.

f) L'absence de « valeur » d'une donnée personnelle isolée

***448.*** Aux États-Unis, l'école d'économie de Chicago, incarnée par le Professeur Posner, considère que, « dans la mesure où les données personnelles ne sont pas produites par les utilisateurs, on ne pourrait pas leur attribuer un droit de propriété. La création de valeur ne supposerait aucun effort de la part des individus puisqu'elle découle des informations qu'elle génère parfois à leur insu. Ce droit devrait plutôt être consenti à ceux qui investissent pour la valorisation de ces données, c'est-à-dire les exploitants, sites, plateformes et autres réseaux sociaux »[1061]. Il s'agirait, ici, de considérer que « la valeur ajoutée est apportée par les collecteurs des données (site internet, plateformes) qui transforment cette matière brute par leur industrie, dès lors du fait des efforts mis en œuvre pour collecter, traiter, exploiter nos données, ils en deviendraient propriétaires »[1062]. Si ce postulat est empreint de réalisme quant à l'affirmation du principe que la donnée brute, isolée, c'est-à-dire celle fournie par un seul individu, ne dispose que de très peu de valeur et d'intérêt contrairement à la donnée agrégée (celle qui va être valorisée par d'autres données (big data)) ; en revanche, l'affirmation d'un droit de propriété au bénéfice des exploitants est sujette à discussion et rejoint, en conséquence, le débat autour de la propriété des données.

***449.*** Quant à la valorisation des données personnelles, la doctrine a révélé qu'« une donnée brute, une donnée isolée, une donnée qui n'est pas mise en corrélation avec d'autres n'a que très peu de valeur en soi »[1063]. À ce titre, le Conseil d'État avait considéré sur ce point que « la valeur des données d'un seul individu est très limitée. En outre, même si le prix des données est voué à augmenter de manière considérable, il n'en demeure pas moins que la valeur de l'actif conférée

[1059] Ibid.

[1060] Benabou V-L., Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? RTD Eur. 2021 p.279.

[1061] Basdevant A., Mignard J-P., L'empire des données, essai sur la société, les algorithmes et la loi, p.123, *op. cit.*.

[1062] Ibid.

[1063] Ibid.

à chaque individu demeurerait faible »[1064]. Cette prise de position doctrinale et jurisprudentielle vient en opposition avec l'étude menée aux États-Unis par Monsieur Lanier et des universitaires qui prône l'idée de rémunérer la personne physique en contrepartie de son accord au profit des entreprises pour l'utilisation de ses données personnelles[1065]. Le point de la monétisation des données des personnes au profit de la personne physique a été tranché dans le cadre d'une question posée lors des travaux préparatoires de la directive européenne du 20 mai 2019[1066], dont un des projets prévoyait que ce texte s'appliquerait à « tout contrat par lequel un fournisseur fournit un contenu numérique au consommateur ou s'engage à le faire », en échange duquel « un prix doit être acquitté ou une contrepartie non pécuniaire, sous la forme de données personnelles ou de toutes autres données, doit être apportée de façon active par le consommateur »[1067]. Dans le cadre de son avis sur la directive, le contrôleur européen de la protection des données (CEPD) [1068] a suggéré et « obtenu d'éviter l'utilisation, dans le texte final, de la notion de « données comme contrepartie », afin d'éviter de laisser supposer que l'on considèrerait les informations personnelles « comme une marchandise » (pt 14), insistant sur le fait qu'on ne peut « monétiser et soumettre un droit fondamental à une simple transaction commerciale, même si c'est la personne concernée par les données qui intervient dans la transaction » (pt 18) »[1069]. Par le retrait de cette mention, le texte retire toute ambiguïté quant à la possibilité de recevoir une rétribution pour l'exploitation des données personnelles.

***450.*** Ces arguments issus principalement de la théorie personnaliste du droit à la protection des données contribuent à mettre en échec la thèse de la patrimonialisation des données à caractère personnel et donc de la reconnaissance d'un droit de propriété des données personnelles. Face au rejet, il est proposé ici de renforcer la protection des données personnelles dans les contrats cloud par un droit spécifique, le droit à l'autodétermination informationnelle.

---

[1064] Étude annuelle 2014, Conseil d'Etat, le numérique et les droits fondamentaux, 8 septembre 2014 : https://www.conseil-etat.fr/publications-colloques/etudes/le-numerique-et-les-droits-fondamentaux.

[1065] Lanier J., Arrieta Ibarra I., Goff L., Jimenez Herna´ndez D., Weyl E. G., « Should We Treat Data as Labor? Moving Beyond 'Free' » (traduction en français : " Devrions-nous traiter les données comme de la main-d'œuvre ? Au-delà de la "gratuité") Vol.1 N°1, Mai 2018 : copie électronique disponible sur https://ssrn.com/abstract=3093683.

[1066] Directive (UE) 2019/770 du Parlement Européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques.

[1067] Basdevant A., Mignard J-P., L'empire des données, essai sur la société, les algorithmes et la loi, Don Quichotte éditions, mars 2018, p.120.

[1068] CEPD - EDPS, Avis 4/2017 sur la proposition de directive concernant certains aspects des contrats de fourniture de contenu numérique, 14 mars 2017 : https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_fr.pdf.

[1069] Basdevant A., Mignard J-P., L'empire des données, essai sur la société, les algorithmes et la loi, Don Quichotte éditions, mars 2018, p.120.

## Section 2 : La proposition d'une protection des données par le droit à l'autodétermination informationnelle

***451.*** Cette étude nous amène à considérer que le concept de propriété (tel qu'appréhendé en droit civil français) est inadapté à la protection des données dans les contrats de cloud computing et qu'il faille davantage se tourner vers la théorie personnaliste afin de renforcer le cadre de la protection des données dans les contrats de cloud computing. Il apparaît, en effet, que la théorie personnaliste est plus en phase avec les impératifs des personnes physiques (en développant la sécurisation des données par la consécration de droits) et du marché économique (en favorisant le développement de l'innovation dans tous les domaines économiques et la compétitivité par le jeu de la libre circulation des données).

***452.*** À l'issue de cette étude sur la propriété des données, il est pris position de rejoindre la thèse personnaliste du droit à la protection des données. Nous suivons à ce titre les recommandations du Conseil d'État qui préconise de renforcer le droit à la protection des données personnelles « par le droit à l'autodétermination plutôt que comme un droit de propriété (proposition n° 1) »[1070]. Selon le Conseil d'État, « la reconnaissance du droit de propriété ne permettrait pas en effet de rééquilibrer la relation entre les individus et les acteurs économiques et compliquerait l'exercice de la régulation par les pouvoirs publics »[1071]. Pour le Conseil d'État, le droit des données personnelles doit être rattaché à la personne elle-même et non entrer dans le champ du droit de la propriété. Nous allons porter, donc, davantage notre étude sur le droit à l'autodétermination informationnelle qui semble plus à même de convenir au renforcement de la protection des données dans les contrats de cloud computing.

***453.*** **Plan.** Pour renforcer la protection des données à caractère personnel dans les contrats cloud, il est envisagé d'étudier la consécration d'un droit à l'autodétermination informationnelle (A) suivi de la mise en œuvre de ce droit dans le contrat cloud (B).

[1070] Étude annuelle 2014, Conseil d'Etat, le numérique et les droits fondamentaux, 8 septembre 2014 : https://www.conseil-etat.fr/publications-colloques/etudes/le-numerique-et-les-droits-fondamentaux.

[1071] Ibid.

## A) Le renforcement de la protection des données personnelles par la consécration du droit à l'autodétermination informationnelle

***454.*** **Plan.** Dans cette partie, il est envisagé de déterminer le droit à l'autodétermination informationnelle (1) ainsi que ses prérogatives au profit de la personne physique pour le renforcement de la protection de ses données personnelles dans les contrats de cloud computing (2).

### 1) La détermination du droit à l'autodétermination informationnelle

***455.*** Parmi les auteurs affirmant qu'il n'existe pas pour l'heure de droit à la propriété des données, A. Bensoussan, indique à ce sujet que « nous devons au moins créer « le droit à la souveraineté, à l'autodétermination par l'utilisateur de ses droits. Le droit à la souveraineté est sûrement un droit fondamental, un droit naturel qui permet au-delà de la propriété, nonobstant la propriété ou malgré le fait qu'il n'y ait pas de propriété, de pouvoir effectivement contrôler ses données et décider de leur utilisation »[1072]. Cet auteur met clairement en évidence la nécessité de conférer des prérogatives aux « titulaires » des données. Ainsi s'agirait-il de conférer *a minima* « un droit à la souveraineté » et « un droit à l'autodétermination », dont les concepts juridiques sont empruntés au droit constitutionnel et au droit international. Le « droit à la souveraineté » fait allusion au pouvoir du peuple, lequel est souverain dans un état démocratique, tel qu'il est affirmé à l'article 3 de la constitution de 1958[1073], traduit par le principe du gouvernement du peuple, par le peuple et pour le peuple. Quant au « droit à la détermination » appelé également « le droit des peuples à disposer d'eux-mêmes », inscrit à l'article 1er de la Charte des Nations unies de 1945[1074], est un concept développé et utilisé après la Seconde Guerre mondiale pour revendiquer la décolonisation et désignant, en substance, que chaque peuple devrait disposer du droit de déterminer la forme de son régime politique, et ce sans influence d'une autre puissance étrangère. Appliqué à la matière du cloud computing, il s'agirait de permettre à la personne concernée d'avoir un « droit de contrôle » sur ses données à caractère personnel ainsi que la faculté pour elle de déléguer si elle souhaite certaines prérogatives dont elle dispose sur sa donnée sans interférence de la puissance publique ou des acteurs privés. Ce principe permet d'attribuer à chacun le pouvoir de décider, en toute autonomie, l'usage de ses données personnelles.

[1072] Article de Bensoussan A., « Du big data au fast data, le nouvel écosystème de la data », 2 juin 2017, publié sur le site d'information www.contrepoints.org. V. également, Bensoussan A., Statut juridique des données vers un droit du big data, 29 juin 2017, disponible sur https://www.alain-bensoussan.com/avocats/statut-donnees-droit-du-big-data/2017/06/29/.

[1073] V. art. 3 de la Constitution française de 1958.

[1074] V. art. 1er alinéa 2 de la Charte des Nations Unies de 1945.

***456. La consécration jurisprudentielle du droit à l'autodétermination informationnelle***. Le droit à l'autodétermination informationnelle a, d'abord, été le fruit d'un apport jurisprudentiel. C'est la Cour constitutionnelle allemande qui, en 1983, a fait ressortir le principe du droit à l'autodétermination informationnelle à partir de la combinaison des articles 1er concernant la dignité de l'homme et 2 à propos du droit au libre développement de sa personnalité[1075]. Dans la continuité de cette jurisprudence, le Conseil d'État a, en 2014, préconisé "de concevoir le droit à la protection des données personnelles comme un droit à « l'autodétermination informationnelle », c'est-à-dire le droit de l'individu de décider de la communication et de l'utilisation de ses données à caractère personnel"[1076]. Dans le cadre de ses propositions, le modèle du droit de propriété est écarté au profit du droit à l'autodétermination informationnelle. La préférence pour le droit à l'autodétermination informationnelle est prise au motif que « là où le droit de propriété prétend faire des individus des gestionnaires d'un patrimoine, le droit à l'autodétermination informationnelle rappelle qu'ils doivent demeurer en mesure de décider de leur existence. L'un se situe sur le plan de l'avoir, l'autre sur celui de l'être »[1077]. Par cette déclaration, le Conseil d'État affiche clairement son parti pris pour la thèse personnaliste de la protection des données. Il en résulte que le droit à l'autodétermination informationnelle est un droit de la personnalité, c'est-à-dire attaché à la personne physique. Il est affirmé que ce droit a pour objet de garantir « la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel »[1078].

***457. Une divergence doctrinale.*** Le droit à l'autodétermination informationnelle a été défini, par la doctrine, comme étant « le droit d'une personne de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant »[1079]. Il en résulte de ces définitions, que le droit à l'autodétermination informationnelle peut être conçu comme « une finalité, et peut s'entendre comme la possibilité de transcrire et de maîtriser son identité dans l'espace numérique »[1080]. Il s'agirait de considérer que cette autonomie s'accompagne du droit pour chacun « de savoir ce que l'on sait de lui »[1081]. Certains auteurs en ont déduit de cette

---

[1075] Cour constitutionnelle allemande, BVerf GE 65, 1, Volkszahlung, 15 décembre 1983, *in* Basdevant A., Mignard J-P, L'empire des données, essai sur la société, les algorithmes et la loi, Don Quichotte éditions, mars 2018, p.128.

[1076] Étude annuelle 2014, Conseil d'Etat, le numérique et les droits fondamentaux, 8 septembre 2014 : https://www.conseil-etat.fr/publications-colloques/etudes/le-numerique-et-les-droits-fondamentaux.

[1077] Ibid.

[1078] Ibid.

[1079] Lassalle M., Droit à l'autodétermination informationnelle - La réparation des atteintes au droit à l'autodétermination informationnelle, Communication Commerce électronique n° 2, Février 2021, étude 4.

[1080] Basdevant A., Mignard J-P., L'empire des données, essai sur la société, les algorithmes et la loi, Don Quichotte éditions, mars 2018, p.129.

consécration qu'il s'agissait « d'un renforcement légal des droits de la personne dans une logique « d'empowerment »[1082] ou « d'empouvoirement »[1083] de l'internaute »[1084]. Un débat doctrinal est apparu sur le point de savoir si le droit à l'autodétermination informationnelle devait être considéré comme ajoutant un « nouveau » droit au profit de la personne physique[1085]. Sur ce point, le Conseil d'État, dans son rapport, ne l'envisageait pas comme un nouveau droit s'ajoutant à ceux déjà existants, mais, d'attribuer une place centrale au profit de la personne dans ce dispositif informatique et libertés. Précisément, il est affirmé que ce droit ne devrait pas être défini comme un droit supplémentaire s'ajoutant aux autres droits (droit d'information, droit d'accès...), mais comme un principe donnant sens à tous ces droits, ceux-ci tendant à le garantir et devant être interprétés et mis en œuvre à la lumière de cette finalité[1086]. Ce droit est, ainsi, considéré comme étant un objectif permettant de renforcer la protection des données personnelles[1087]. Il s'agit, pour le Conseil d'État, d'attribuer à ce droit le rôle « d'aiguillon, tant pour les pouvoirs publics que pour les individus »[1088]. À cette fin, la personne physique doit disposer de moyens lui permettant « de demeurer libre de conduire son existence, dans une société où le numérique prend une place croissante, qui l'amène à laisser, de plus en plus souvent, trace de ses données personnelles »[1089]. Une place centrale est donc, accordée, au renforcement de la protection des données personnelles dans le cadre de l'utilisation de services technologiques. Le renforcement de ces moyens se traduit notamment, ici, par une meilleure information de la personne. Le postulat défendu est de considérer que ce n'est que si la personne physique dispose des informations qu'elle peut avoir la capacité d'agir pour la protection de ses

---

[1081] Hurpy H., Fonction de l'autonomie personnelle et protection des droits de la personne humaine dans les jurisprudences constitutionnelles et européennes, thèse de sciences juridiques et politiques soutenue le 27 juin 2013, à l'université d'Aix en Provence.

[1082] Cluzel-Métayer L., « La loi pour une République numérique : l'écosystème de la donnée saisi par le droit », *AJDA* 2017, p. 340, spéc. IIA) ; B. Thieulin, « Gouverner à l'heure de la révolution des pouvoirs », *Pouvoirs* 2018/1, n° 164, p. 19, spéc. p. 19-20 et p. 28.

[1083] Berthet C., Zolynski C., « L'empouvoirement" des citoyens de la République numérique regards sur une réforme en construction », *RLDI* 2018/1, n° 144, p. 60, spéc. n° 14.

[1084] Netter E., Ndior V., Puyraimond J-F, Vergnolle S. Regards sur le nouveau droit des données personnelles. Centre de droit privé et de sciences criminelles d'Amiens. 2019, 979-10-97323-05-9. hal-02357967.

[1085] Lepage A., La protection contre le numérique : les données personnelles à l'aune de la loi pour une République numérique - Le droit civil à l'ère du numérique, actes du colloque du Master 2 Droit privé général et du Laboratoire de droit civil - Paris II - 21 avril 2017, La Semaine Juridique, Lexisnexis - Décembre 2017, page 37.

[1086] Étude annuelle 2014, Conseil d'Etat, le numérique et les droits fondamentaux, 8 septembre 2014 : https://www.conseil-etat.fr/publications-colloques/etudes/le-numerique-et-les-droits-fondamentaux.

[1087] Ibid.

[1088] Ibid.

[1089] Ibid.

données personnelles. Il s'agirait, ici, de satisfaire à « l'aspiration croissante des individus à « l'autonomie de la décision »[1090].

***458. La consécration légale du droit à l'autodétermination informationnelle***. La consécration de ce principe à l'autodétermination informationnelle (intégrant le droit de contrôle sur les données et le droit de décision sur l'utilisation des données) repose sur le droit fondamental à la protection des données à caractère personnel dont les principes en découlant sont retranscrits dans plusieurs textes[1091]. Ce droit à l'autodétermination informationnelle a été consacré par la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique à l'article 54[1092], laquelle a modifié l'article 1er de la loi du 6 janvier 1978 afin d'intégrer ce droit à l'autodétermination informationnelle[1093]. Cet ajout (dans la loi du 6 janvier 1978) trouve son fondement dans une proposition faite par le Conseil d'État dans le cadre de son étude annuelle sur l'autodétermination informationnelle[1094]. Il est consacré que « toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi »[1095]. Puis, le règlement européen sur la protection des données a intégré dans ses dispositions les illustrations du droit à l'autodétermination informationnelle[1096]. Ce droit à l'autodétermination informationnelle, ainsi, consacré permet de conférer au profit de la personne physique, un droit à la libre disposition de ses données[1097]. Ces dispositions légales entérinent, ainsi, la thèse personnaliste de la protection des données personnelles, telle que promue par le Conseil d'État et ce « en renforçant les droits de la personne sur l'usage de ses données »[1098].

---

[1090] Ibid.

[1091] V. supra n° 107.

[1092] V. art. 54 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

[1093] V. art. 1er de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par l'ordonnance n°2018-1125 du 12 décembre 2018.

[1094] Conseil d'État, Étude annuelle 2014, Le numérique et les droits fondamentaux, p. 264 et s.

[1095] V. art. 1er alinéa 2, loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; cet alinéa second de l'article 1er de cette loi a été modifié par l'ordonnance n° 2018-1125 du 12 décembre 2018 en application du décret n° 2019-536 du 29 mai 2019 suite à l'entrée en vigueur du RGPD comme suit « Les droits des personnes de décider et de contrôler les usages qui sont faits des données à caractère personnel les concernant et les obligations incombant aux personnes qui traitent ces données s'exercent dans le cadre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 et de la présente loi ».

[1096], V. considérants 7, 11 et 68 et les articles 7, 8, 12, 13, 14, 17, 18, 19 et 20 du RGPD, dans Netter E., Ndior V., Puyraimond J-F, Vergnolle S. Regards sur le nouveau droit des données personnelles. Centre de droit privé et de sciences criminelles d'Amiens. 2019, 979-10-97323-05-9. hal-02357967.

[1097] V. art. 1er, alinéa 2, loi n° 78-17 du 6 janvier 1978.

[1098] Netter E., Ndior V., Puyraimond J-F, Vergnolle S. Regards sur le nouveau droit des données personnelles. Centre de droit privé et de sciences criminelles d'Amiens. 2019, 979-10-97323-05-9. hal-02357967.

***459. La nature juridique du droit à l'autodétermination informationnelle.*** Ce droit à l'autodétermination informationnelle permet de conférer à la personne physique un droit de contrôle et un droit de décision sur l'utilisation de ses données à caractère personnel. Ce droit à l'autodétermination informationnelle est un droit purement personnel[1099] puisqu'il est fondé sur le droit fondamental à la protection des données à caractère personnel qui donne naissance à une déclinaison d'autres droits. Ce droit de contrôle et de décision sur l'usage des données est considéré comme étant un attribut de la personnalité[1100]. La consécration de ce droit s'inscrit dans le cadre de la thèse personnaliste du droit à la protection des données[1101].

***460. Le droit à l'autodétermination informationnelle versus le droit de contrôle.*** Concernant l'importance de la communication des informations par les prestataires au profit des personnes physiques, la doctrine la relie au droit de contrôle. Il est mis en avant l'idée que "l'essentiel réside dans la capacité de contrôler la divulgation des informations personnelles ("control over personal information"), permettant à l'individu de déterminer quand, comment et dans quelle mesure souhaite-t-il dévoiler ces informations[1102]. Cette position doctrinale envisage, ainsi, l'effectivité du droit à l'autodétermination informationnelle par l'exercice, au profit de la personne physique, du droit de contrôler la divulgation de ses données personnelles. Il en résulte de cette analyse que le droit à l'autodétermination informationnelle intègre deux volets, le droit de contrôle sur les données et le droit de décision sur l'utilisation des données.

***461.*** Il est envisagé, à présent, de déterminer quelles sont les prérogatives attachées au droit à l'autodétermination informationnelle.

---

[1099] Basdevant A. et Mignard JP., l'empire des données - essai sur la société, les algorithmes et la loi, Don Quichotte éditions, mars 2018, p.113 : « Les pays latins dont la France ont une conception personnaliste des données à la différence des États-Unis qui ont une conception réaliste des données laquelle s'accommode davantage d'une patrimonialisation des données ». Concernant la théorie de la patrimonialisation des données qui prône une marchandisation des données, V. conception utilisatrice de l'école de Chicago, Richard V. et Poster A., An economic Theory of Privacy, Regulation, vol.2, n°19, 1978.

[1100] Cousin A, « La Data au cœur du projet de loi pour une République numérique », D. 2018, p. 2176.

[1101] V. *supra* n° 434.

[1102] Westin A., Privacy, and freedom, Atheneum, 1967. V. également, Saint-Aubin Th., « Les nouveaux enjeux juridiques des données (big data, web sémantique et linked data ») : les droits de l'opérateur des données sur son patrimoine numérique informationnel », Revue Lamy droit de l'immatériel, 2014.

**2) La détermination des prérogatives du droit à l'autodétermination informationnelle**

***462. Le droit à l'information.*** Pour rendre effectif le droit à l'autodétermination informationnelle, la personne physique doit disposer des informations concernant la collecte et le traitement de ses données personnelles. Ce droit à l'information de la personne physique auprès de laquelle sont recueillies les données à caractère personnel est de longue date ancré dans la loi du 6 janvier 1978, mais il s'est étendu avec la loi du 7 octobre 2016[1103] et le RGPD[1104]. Il s'agit d'une obligation mise à la charge du responsable du traitement des données (ici le prestataire de services cloud) qui doit fournir à la personne concernée des informations relatives à l'identité et les coordonnées du responsable du traitement, les finalités du traitement, la base juridique du traitement, les intérêts légitimes poursuivis, les destinataires ou les catégories de destinataires des données à caractère personnel[1105]. L'exhaustivité de ce droit à l'information permet de conférer aux personnes physiques la connaissance du périmètre des informations dont elles sont légitimement en droit de demander au prestataire de services cloud. Ces informations doivent être délivrées dans un délai raisonnable tout en ne dépassant pas un mois eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées[1106]. La fixation d'un délai maximal pour la délivrance de ces informations contribue, ainsi, au renforcement du droit à l'autodétermination informationnelle et donc du droit à la protection des données à caractère personnel. La délivrance de ces informations est une obligation positive à la charge du prestataire de services cloud dès lors que le contrat cloud prévoit un traitement des données. Également, la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique a créé une obligation de loyauté pour les plateformes en ligne, laquelle implique une obligation renforcée d'information à l'égard de l'utilisateur et permettrait ainsi de compenser le déséquilibre contractuel entre le fournisseur de services cloud et son client[1107]. C'est parce que le client, personne physique, est en mesure de recevoir les informations concernant la collecte et le traitement de ses données qu'il sera en mesure d'exercer son droit à l'autodétermination informationnelle (c'est-à-dire son droit de contrôle et son droit de décision

[1103] Avec la loi du 7 octobre 2016, la personne doit être informée, au moment de la collecte des données, de la durée de conservation de celles-ci. Cette loi a anticipé la transposition du règlement européen sur ce point (RGPD, art. 13(2), a)).

[1104] V. article 13 et 14 du RGPD.

[1105] V. en ce sens CE, 24 août 2011, n° 336382, Société HSBC Private Bank Suisse SA : Le CE rappelle le principe selon lequel les responsables de traitement sont tenus de communiquer aux personnes concernées les caractéristiques essentielles du traitement ainsi que leurs droits.

[1106] Article 14 du RGPD.

[1107] Basdevant A., Mignard J-P., L'empire des données, essai sur la société, les algorithmes et la loi, Don Quichotte éditions, mars 2018, p.129.

sur l'utilisation de ses données) et ainsi renforcer la protection de ses données personnelles dans le cadre de l'exécution du contrat cloud.

***463. Le droit d'accès aux données.*** Outre la nécessité de jouir du droit à l'information pour être en mesure d'exercer son droit à l'autodétermination informationnelle, l'individu doit bénéficier du « droit d'accès aux données »[1108] et ce conformément à l'article 15 du RGPD. Il est affirmé à l'article 39 de la loi informatique et libertés de 1978 que « tout sujet concerné par un traitement de données nominatives l'intéressant bénéficie d'un « droit d'accès » qui lui permet d'obtenir communication des informations traitées[1109]. Ce droit d'accès vise les informations sur support papier[1110] ainsi que sur support informatisé et cela inclut les enregistrements audios, les vidéos[1111] et les données de géolocalisation[1112]. Concernant la mise en œuvre de ce droit dans le cadre d'un contrat de cloud computing, il faut distinguer, d'une part, le droit à l'accessibilité aux informations traitées par le prestataire[1113], lequel se traduit par le droit d'obtenir ces informations et d'autre part, le droit d'accès aux données stockées dans le cloud, lequel se manifeste par une obligation à la charge du prestataire de services cloud de mettre à la disposition de l'utilisateur les outils techniques garantissant cet accès. La première obligation concerne précisément ce que l'on appelle « le droit d'accès aux données personnelles »[1114] alors que la seconde concerne davantage « la disponibilité » du service cloud. Cette obligation de disponibilité est précisée dans une clause spécifique intitulée «  disponibilité et autres niveaux de services » qui peut figurer dans un document en annexe (soit le Plan Assurance Qualité, soit dans le SLA) ou dans le corps du contrat cloud laquelle contient à tire d'exemple « les plages d'accès aux Services, les éventuelles suspensions de services pour raison de maintenance et leur durée maximale ainsi que les procédures d'information préalable du Client, les modes d'accès possibles aux Services par le Client, ainsi que l'utilisation des identifiants de connexion par les utilisateurs finaux, les règles de confidentialité de ces identifiants et la procédure à suivre en cas de perte ou de vol de

[1108] Mattatia F., Synthèse du futur règlement européen sur les données personnelles (1re partie) : principaux généraux et obligations du responsable de traitement : RLDI 2016/126, no 3985, p. 39). V. également Bounedjoum A., Réforme européenne des données personnelles : les nouveautés pour les droits des personnes : JCP E 2016, 1327.

[1109] Article 39, loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[1110] CNIL, Guide « Droit d'accès », 2016, p. 6

[1111] CNIL, Guide « Droit d'accès », 2016, p. 5.

[1112] CNIL, délib. n° 2012-213, 22 juin 2012.

[1113] Telles que les données collectées en matière de gestion de clientèle : Uzan-Naulin J. et Perray R., La nouvelle norme simplifiée de la CNIL en matière de clients, prospects et vente en ligne : entre convergence, cohérence et conformité, Comm. com. électr. 2017, étude 2.

[1114] L'entrave au droit d'accès constitue une contravention de la cinquième classe répréhensible pénalement (C. pén., art. R. 625-11).

ceux-ci »[1115]. Dans les deux cas, il s'agit d'une obligation positive à la charge du prestataire et devront être intégrées dans le contrat par des clauses spécifiques.

***464. Le droit de rectification des données.*** Le droit à l'autodétermination contient, également, le droit de rectification qui permet à la personne physique d'exiger de la part de son prestataire la rectification de ses données à caractère personnel. Précisément, il s'agit du droit pour la personne concernée par le traitement d'obtenir du responsable du traitement la rectification des données lorsque celles-ci sont inexactes ou incomplètes[1116]. Dès lors que le prestataire de services traite certaines données du client (personne physique), ce dernier est en droit de demander à son prestataire de services de rectifier certaines données. Dans le cadre d'un contrat de cloud computing, ce droit de rectification ne concerne que les données faisant l'objet d'une collecte et d'un traitement par le prestataire de services cloud et non celles qui sont hébergées dans l'infrastructure cloud. En cas de demande de modification par la personne concernée, la Cour de cassation[1117] avait précisé qu'il est possible de ne pas faire droit à la demande de rectification sur ses données personnelles lorsque par exemple en cas d'impossibilité technique. La Cour a considéré que la Banque Postale « dès lors qu'elle avait justifié de l'impossibilité technique de porter des accents sur les majuscules des noms patronymiques, se trouvait déchargée de son obligation de rectifier les données à caractère personnel de l'un de ses clients qu'elle traitait ». En tout état de cause, ce droit de rectification de la personne concernée constitue une prérogative lui permettant de renforcer la protection de ses données personnelles.

***465. Le droit à la limitation du traitement des données.*** Dans le cadre de l'exercice du droit à l'autodétermination informationnelle, la personne physique dispose du « droit à la limitation du traitement » dont les contours ont été définis par la loi[1118] ; il s'agit du droit d'obtenir du responsable du traitement la limitation du traitement lorsque l'exactitude des données est contestée, le traitement est illicite, les données ne sont plus nécessaires pour le responsable du traitement, mais elles demeurent utiles pour la constatation, l'exercice ou la défense de droits en justice ou la personne concernée s'est opposée au traitement[1119]. Ce droit à la limitation du traitement peut recevoir une application dans le cadre d'un contrat de cloud computing dès lors

[1115] Formulaires ProActa droit de l'immatériel, Conditions d'utilisation du logiciel en mode Saas, 2022, LAMYLINE.

[1116] Article 16 du RGPD : « La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire ».

[1117] Cass. 1re civ., 4 mai 2012, n° 10-27.208, Gaz. Pal., 17 mai 2012, no 138, p. 13.

[1118] Maisnier-Boché L., Droit à l'effacement, à la rectification, à la limitation et droit d'opposition dans le Règlement européen : Comm. com. électr. 2018, comm. 14.

[1119] V. art. 18 du RGPD.

que sont prévus une collecte et un traitement de données personnelles. À l'instar des autres droits, le droit à la limitation du traitement n'est pas absolu, il est prévu des exceptions légales telles que la constatation, l'exercice, ou la défense de droits en justice, ou pour la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public de l'Union ou d'un autre État membre. En tout état de cause, ce droit contribue, à l'instar des autres droits étudiés dans cette partie, à renforcer l'effectivité du droit à l'autodétermination informationnelle et, ainsi, permettre un renforcement de la protection des données dans les contrats de cloud computing dès lors que ce droit est intégré dans le champ contractuel.

***466. Le droit à l'effacement des données.*** Le droit à l'autodétermination informationnelle comprend, également, un « droit à l'effacement » encore appelé « droit à l'oubli » au profit de la personne physique. Il s'agit du droit pour la personne concernée par le traitement d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement à l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais[1120]. En l'espèce, le RGPD reprend en substance le droit au déréférencement consacré par la Cour de justice de l'Union européenne[1121]. À l'instar des autres droits étudiés, ce droit à l'effacement ou le droit à l'oubli n'est pas absolu[1122], il existe des exceptions à ce principe lorsque notamment ce droit est en conflit avec d'autres droits et libertés fondamentaux. Ainsi, le droit à l'effacement ou le « droit à l'oubli » peut être limité ou remis en cause lorsque le traitement est nécessaire à l'exercice du droit à la liberté d'expression et d'information, pour respecter une obligation légale, pour exécuter une mission d'intérêt public, pour des motifs d'intérêt public dans le domaine de la santé publique, à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, à la constatation, à l'exercice ou à la défense de droits en justice[1123]. Ce droit à l'effacement ou ce droit à l'oubli est applicable dans le cadre d'un contrat de cloud computing. Concrètement, le client (personne physique) pourra mettre un terme au contrat de cloud computing sous réserve du respect des conditions de résiliation du contrat et demander la suppression de son compte cloud et l'effacement de toutes ces données stockées dans le cloud. Le client pourra lui-même réaliser l'effacement de ses données dans le cloud s'il dispose des

[1120] V. art. 17 du RGPD.

[1121] CJUE, 13 mai 2014, affaire n° C-131/12, Google Spain SL, Google Inc. c/ Agencia Española de Protección de Datos (AEPD) et Mario Costeja González. Pour une application de la jurisprudence européenne par les juridictions françaises, v. TGI Paris, ord. réf., 16 sept. 2014 M. et Mme X. et M. Y. c/Google France.

[1122] Jouffin E., Lemarteleur X. et Gibon M.-N., Le Règlement sur la Protection des données : les 10 Commandements à connaître pour passer de la théorie à la pratique : RD bancaire et fin. 2016, étude 18, p.1.

[1123] Ibid.

outils technologiques pour le faire ou à défaut d'exiger du prestataire qu'il les efface de manière effective au terme du contrat de cloud computing.

***467. Le droit d'obtenir une notification concernant le traitement de ses données.*** Le droit à l'autodétermination informationnelle permet, également, de conférer à la personne physique le droit d'obtenir une notification. Précisément, la personne physique a le « droit d'obtenir une notification concernant la rectification ou l'effacement de données, ou la limitation du traitement ». Ce droit exige du responsable du traitement qu'il notifie aux personnes concernées toute rectification, ou tout effacement de données à caractère personnel ou toute limitation du traitement[1124]. Dans le cadre d'un contrat de cloud computing, le client pourra actionner son droit de recevoir des notifications du prestataire de services cloud à la suite d'une rectification ou l'effacement de données et de tout incident pouvant affecter la sécurité des données.

***468. Le droit d'opposition de la personne physique.*** Le droit à l'autodétermination informationnelle permet, aussi, d'attribuer à la personne physique un « *droit d'opposition* »[1125] ; il s'agit du droit pour la personne concernée de s'opposer à tout moment à un traitement de ses données à caractère personnel. Ce droit à l'instar des autres droits n'est pas absolu et est assorti d'exceptions[1126] notamment lorsqu'il existe des motifs légitimes, tels que nous les avons abordés ci-dessus, qui prévalent sur les intérêts et les droits et libertés de la personne concernée. L'existence des motifs légitimes est appréciée de manière stricte par les juges. Le Conseil d'État[1127] a décidé d'annuler les dispositions de la Base élève 1er degré[1128] au motif qu'elles interdisaient aux personnes concernées de faire application du droit d'opposition pour des motifs légitimes. Également, les juges judiciaires statuent dans le même sens en considérant que « la société Google Inc, bien qu'implantée aux États-Unis, devait permettre à la personne dont les données sont traitées d'exercer son droit d'opposition »[1129]. Dans le cadre d'un contrat de cloud computing, le client peut exercer son « droit d'opposition » afin de s'opposer à tout moment à un traitement de ses données à caractère personnel. Ainsi, dans le cadre d'un contrat de cloud ayant prévu une licence de collecte et de traitement des données, le client (personne physique) conserve la possibilité de s'opposer au traitement de ses données à caractère personnel.

---

[1124] V. article 19 du RGPD.

[1125] V. article 21 du RGPD.

[1126] Maisnier-Boché L., Droit à l'effacement, à la rectification, à la limitation et droit d'opposition dans le Règlement européen : Comm. com. électr. 2018, comm. 14.

[1127] CE, 19 juill. 2010, nº 317182, AJDA 2010, p. 1454, obs. de Montecler M.-C.

[1128] Il s'agit d'une application d'aide à l'inscription des élèves et à la gestion pour les directeurs d'école et les mairies de France laquelle a commencé à être déployée en 2007.

[1129] TGI Montpellier, ord. réf., 28 oct. 2010, Marie C. c/ Google France et Inc.

***469. Le droit à la portabilité des données.*** Ce droit à l'autodétermination informationnelle permet de conférer à la personne physique le droit d'exiger de recevoir, du responsable du traitement, ses données dans un format adapté et structuré lui permettant de faciliter leurs transmissions à un autre responsable du traitement[1130]. Ce droit à la portabilité, contrairement au droit d'accès, ne consiste ainsi pas « à communiquer les données dans un format lisible par la personne humaine, à des fins de vérification des conditions du traitement, mais dans un format lisible par machine, aux fins de permettre de nouvelles utilisations des mêmes données »[1131]. Ce droit constitue l'incarnation de la logique du droit à l'autodétermination informationnelle, « poursuivie par le RGPD et déjà introduite par la loi « Lemaire » à l'alinéa 2 de l'article 1er de la loi « Informatique et libertés », selon laquelle l'individu doit conserver le « contrôle » (RGPD, consid. n° 68) tout à la fois la circulation et la réutilisation de ses données »[1132]. Le droit à la portabilité ne s'applique qu'à l'égard de données personnelles (exclusion des données anonymisées) faisant l'objet d'un traitement « automatisé » (exclusion des données traitées de manière exclusivement manuscrite) qui repose soit sur le consentement de la personne concernée soit sur l'exécution d'un contrat auquel cette dernière est partie et ont été fournies « sciemment et activement par la personne concernée » ou découlant « de l'observation de l'activité » des individus[1133] (exclusion des données enrichies[1134] par le responsable de traitement). À l'instar des autres droits, le droit à la portabilité permet de renforcer le droit à la protection des données puisqu'il offre une prérogative au profit du client non négligeable, celle de récupérer ses données stockées dans un format adapté et structuré. Par la consécration de ce droit à la portabilité des données, la personne physique détient la maîtrise sur ses données stockées dans le cloud en choisissant par exemple de les récupérer dans un format adapté et puis de choisir, le cas échéant, un nouveau prestataire de services cloud pour les stocker.

***470.*** Si le droit à l'autodétermination informationnelle, intégrant les prérogatives issues du droit fondamental à la protection des données à caractère personnel, permet de renforcer la protection

---

[1130] V. article 20 du RGPD.

[1131] Griguer M., Droit d'accès, droit à la portabilité : quelles différences ? : Comm. com. électr. 2018, dossier 14.

[1132] Le Lamy droit du numérique (Guide), Partie 6, Titre 7 Comment gérer un traitement de données personnelles ? Chapitre 1 Quelle est la portée de la réglementation relative à la protection des données personnelles ? Section 2 Quand s'applique la réglementation relative à la protection des données personnelles ? § 1. Quel est le champ d'application matériel de la réglementation relative à la protection des données personnelles ? 2021, Lamyline.

[1133] Groupe de l'article 29, Lignes directrices relatives au droit à la portabilité des données, 5 avr. 2017, WP 242 rév. 01, p. 11

[1134] Il s'agit de données « déduites » ou « dérivées » du fait « d'une analyse subséquente » de sa part, en ce qu'elles « sont générées par [lui] (au moyen des données observées ou directement fournies comme intrants), telles qu'un profil d'utilisateur créé par l'analyse des données brutes collectées à partir d'un compteur intelligent » ou résultant « d'une appréciation relative à la santé d'un utilisateur » : Groupe de l'article 29, Lignes directrices relatives au droit à la portabilité des données, 5 avr. 2017, WP 242 rév. 01, p. 12 et 13.

des données personnelles, encore faut-il que ces prérogatives soient intégrées dans le contrat de cloud computing.

## B) Le renforcement de la protection des données personnelles par l'intégration des prérogatives du droit à l'autodétermination informationnelle dans le contrat cloud

***471.*** Si le droit à l'autodétermination informationnelle intègre le droit de contrôle sur les données et le droit de décision sur l'utilisation des données, il contient, en outre, plusieurs prérogatives au profit des personnes physiques, lesquelles devront rentrer dans le champ contractuel afin de renforcer la protection des données personnelles dans les contrats de cloud computing. Il est envisagé dans cette partie d'effectuer une proposition de rédaction de clauses permettant d'intégrer ces prérogatives dans le contrat cloud afin de rendre effective la protection des données personnelles.

***472.*** À ce titre, il est proposé, ci-après, une clause qui communique les informations à la personne physique concernant les prérogatives dont elle dispose dans le cadre de l'exécution de son contrat de cloud computing ; il s'agit du droit à l'information, du droit d'accès, du droit de rectification, du droit à la limitation du traitement, du droit à l'effacement ou du droit d'oubli, du droit d'obtenir une notification, du droit d'opposition, du droit à la portabilité :

***473.*** « Aux fins de gestion de votre prestation de services de cloud computing, nous sommes amenés à solliciter des données personnelles vous concernant à l'occasion de la conclusion, l'exécution et la rupture de votre contrat de cloud computing. La signature du présent contrat, par vos soins, vaut autorisation pour le Prestataire de collecter, d'enregistrer et de stocker vos données personnelles lesquelles sont nécessaire pour l'exécution de votre contrat (gestion de la commande, du compte client de la relation client, de la facturation, etc..). Il vous est informé que vos données personnelles sont traitées par les services internes du Prestataire et par les partenaires du Prestataire.

Dans le cadre de l'exécution du présent contrat, Vous (client, personne physique) êtes en droit d'obtenir des informations relatives au traitement et à la collecte de vos données personnelles. Conformément au Règlement Général sur la Protection des Données (RGPD) et à la loi modifiée n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, vous pouvez demander à tout moment l'accès aux données à caractère personnel vous concernant, leur rectification, leur effacement et la limitation d'un ou plusieurs traitements particuliers de données vous concernant, dans les conditions prévues par la Réglementation en vigueur. Vous disposez également du droit de modifier ou de retirer, à tout moment, les consentements que

vous nous avez accordés pour le traitement de vos données à caractère personnel. Vous disposez par ailleurs du droit de vous opposer à un traitement de vos données à caractère personnel et du droit à leur portabilité, dans les conditions fixées par la Réglementation. Vos données à caractère personnel peuvent être conservées ou supprimées après votre décès conformément à la Réglementation. Vous disposez du droit de donner instruction au Prestataire de communiquer ces données à un tiers que vous aurez préalablement désigné. Vous pouvez exercer vos droits à tout moment en écrivant à : XXXX ou par courriel à l'adresse suivante : XXXX. Pour toute autre question concernant la collecte et le traitement de vos données personnelles, vous pouvez nous contacter par téléphone au XXXX ou par courriel à l'adresse suivante : XXXX. Nous nous engageons à répondre à vos communications dans un délai maximal de 30 (trente) jours. Pour obtenir davantage d'informations concernant la collecte et le traitement de ses données, et plus généralement la protection des données personnelles, vous avez la possibilité de consulter le document en ligne intitulé « la politique de confidentialité et de protection des données personnelles ».

***474.*** Par ailleurs, il est préconisé, pour une meilleure efficacité, de compléter cette clause générique d'information relative aux prérogatives du droit à l'autodétermination informationnelle par des clauses spécifiques relatives à chacune de ces prérogatives.

***475.*** Il est proposé, ci-après, une clause relative au droit d'accès :

« Dans le cadre de l'exécution de votre contrat de cloud computing, vous disposez d'un droit d'accès aux données vous concernant conformément à la réglementation en vigueur. Ce droit d'accès vous permet d'obtenir de nos Services, la communication de vos informations personnelles ayant fait l'objet d'un traitement. Vous pouvez exercer votre droit d'accès aux données vous concernant en écrivant à : XXXX ou par courriel à l'adresse suivante : XXXX. Nous nous engageons à répondre à vos communications dans un délai maximal de 30 (trente) jours. Pour exercer votre droit d'accès, vous avez la possibilité d'utiliser le formulaire ci-dessous :

*Formulaire pour exercer le droit d'accès et à adresser à l'adresse postale suivante xxxx ou par courriel xxxx : (* informations à remplir par le client)*

Nom : *

Prénom : *

Adresse postale : *

Courriel : *

Numéro de téléphone : *

Référence du contrat : *

Madame, Monsieur,

En application de l'article 15 du Règlement général sur la protection des données (RGPD), je souhaite exercer mon droit d'accès à mes données personnelles. Je vous remercie de bien vouloir m'indiquer si des données me concernant figurent dans vos fichiers et font l'objet d'un traitement automatisé et/ou manuel. En cas de réponse positive, je demande d'obtenir la communication précise de l'ensemble de mes données personnelles faisant l'objet d'un traitement.

En application de l'article 12.3 du RGPD, je vous remercie de m'adresser la communication des informations demandées au plus tard dans un délai d'un mois à compter de la réception de ma demande. En cas de non-réponse ou de réponse incomplète, je me réserve la faculté d'adresser une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL) ».

***476.*** Il est proposé ci-après une clause relative au droit de rectification,

« Dans le cadre de l'exécution de votre contrat de cloud computing, vous disposez d'un droit de rectification de vos données personnelles vous concernant conformément à la réglementation en vigueur. Ce droit de rectification vous permet d'obtenir de nos Services, la rectification de vos données personnelles ayant fait l'objet d'un traitement lorsque celles-ci sont inexactes ou incomplètes. Vous pouvez exercer votre droit de rectification de vos données vous concernant en écrivant à : XXXX ou par courriel à l'adresse suivante : XXXX. Nous nous engageons à répondre à vos communications dans un délai maximal de 30 (trente) jours.

Pour exercer votre droit de rectification, vous avez la possibilité d'utiliser le formulaire ci-dessous :

*Formulaire pour exercer le droit de rectification de vos données personnelles et à adresser à l'adresse postale suivante xxxx ou par courriel xxxx : (* informations à remplir par le client)*

Nom : *

Prénom : *

Adresse postale : *

Courriel : *

Numéro de téléphone : *

Référence du contrat : *

Madame, Monsieur,

En application de l'article 16 du Règlement général sur la protection des données (RGPD), je souhaite exercer mon droit de rectification à mes données personnelles. Je vous remercie de bien vouloir rectifier les données me concernant qui sont inexactes / incomplètes *(veuillez biffer la mention inutile)* lesquelles sont détaillées ci-dessous (*veuillez indiquer précisément votre demande de rectification de vos données*) :

---

---

---

Je vous remercie de bien vouloir me confirmer par écrit de la bonne exécution de la rectification demandée au plus tard dans un délai d'un mois à compter de la réception de ma demande. En cas de non-réponse ou de non-exécution de la rectification, je me réserve la faculté d'adresser un réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

***477.*** Il est proposé, ci-après, une clause relative au droit à la limitation du traitement,

« Dans le cadre de l'exécution de votre contrat de cloud computing, vous disposez d'un droit à la limitation du traitement de vos données personnelles vous concernant conformément à la réglementation en vigueur. Ce droit à la limitation du traitement de vos données personnelles vous permet d'obtenir de nos Services, la limitation du traitement de vos données personnelles dans les cas prévus par la réglementation en vigueur et notamment lorsque l'exactitude des données est contestée, le traitement est illicite, les données ne sont plus nécessaires pour le responsable du traitement. Vous pouvez exercer votre droit à la limitation du traitement des données vous concernant en écrivant à : XXXX ou par courriel à l'adresse suivante : XXXX. Nous nous engageons à répondre à vos communications dans un délai maximal de 30 (trente) jours.

Pour exercer votre droit à la limitation du traitement de vos données personnelles, vous avez la possibilité d'utiliser le formulaire ci-dessous :

*Formulaire pour exercer le droit à la limitation du traitement de vos données personnelles et à adresser à l'adresse postale suivante xxxx ou par courriel xxxx : (* informations à remplir par le client)*

Nom : *

Prénom : *

Adresse postale : *

Courriel : *

Numéro de téléphone : *

Référence du contrat : *

Madame, Monsieur,

En application de l'article 18 du Règlement général sur la protection des données (RGPD), je souhaite exercer mon droit de limitation du traitement de mes données personnelles.

Pour le motif suivant : (*veuillez indiquer une des raisons prévues à l'article 18 du RGPD justifiant la limitation du traitement de vos données*) ----------, je vous remercie de bien vouloir limiter le traitement de mes données concernant les informations suivantes (*veuillez indiquer précisément les données nécessitant une limitation de traitement*) :----------.

Je vous remercie de bien vouloir me confirmer par écrit de la bonne exécution de la limitation du traitement de mes données personnelles au plus tard dans un délai d'un mois à compter de la réception de ma demande. En cas de non-réponse ou de non-exécution de la limitation du traitement de mes données, je me réserve la faculté d'adresser une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL) ».

***478.*** Il est proposé, ci-après, une clause relative au droit à l'effacement ou le droit d'oubli,

« Dans le cadre de l'exécution du contrat de cloud computing, vous disposez d'un droit à l'effacement de vos données personnelles (« droit à l'oubli ») vous concernant conformément à la réglementation en vigueur. Ce droit à l'effacement de vos données personnelles vous permet d'obtenir de nos Services, l'effacement de vos données personnelles dans tous nos fichiers électroniques et manuels. Vous pouvez exercer votre droit à l'effacement de vos données vous concernant en écrivant à : XXXX ou par courriel à l'adresse suivante : XXXX. Nous nous engageons à répondre à vos communications dans un délai maximal de 30 (trente) jours.

Pour exercer votre droit à l'effacement de vos données personnelles (« droit à l'oubli »), vous avez la possibilité d'utiliser le formulaire ci-dessous :

*Formulaire pour exercer le droit à l'effacement de vos données personnelles (« droit à l'oubli ») et à adresser à l'adresse postale suivante xxxx ou par courriel xxxx : (* informations à remplir par le client)*

Nom : *

Prénom : *

Adresse postale : *

Courriel : *

Numéro de téléphone : *

Référence du contrat : *

Madame, Monsieur,

En application de l'article 17 du Règlement général sur la protection des données (RGPD), je souhaite exercer mon droit à l'effacement de mes données personnelles (« droit à l'oubli »). Je vous remercie de bien vouloir procéder à l'effacement de mes données me concernant dans tous vos fichiers électroniques et manuels.

Je vous remercie de bien vouloir me confirmer par écrit de la bonne exécution de l'effacement de mes données personnelles au plus tard dans un délai d'un mois à compter de la réception de ma demande. En cas de non-réponse ou de non-exécution de l'effacement de mes données personnelles, je me réserve la faculté d'adresser une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL) ».

***479.*** Il est proposé ci-après une clause relative au droit d'obtenir une notification,

« Dans le cadre de l'exécution du contrat de cloud computing, vous disposez du droit d'obtenir une notification concernant la rectification, l'effacement, ou la limitation du traitement de vos données personnelles conformément à la réglementation en vigueur. Ce droit de notification vous permet d'obtenir de nos Services, une notification vous informant de la rectification, l'effacement, ou la limitation du traitement de vos données personnelles. Vous pouvez exercer votre droit de notification en écrivant à : XXXX ou par courriel à l'adresse suivante : XXXX. Nous nous engageons à répondre à vos communications dans un délai maximal de 30 (trente) jours.

Pour exercer votre droit de notification, vous avez la possibilité d'utiliser le formulaire ci-dessous :

*Formulaire pour exercer le droit de notification et à adresser à l'adresse postale suivante xxxx ou par courriel xxxx : (* informations à remplir par le client)*

Nom : *

Prénom : *

Adresse postale : *

Courriel : *

Numéro de téléphone : *

Référence du contrat : *

Madame, Monsieur,

En application de l'article 19 du Règlement général sur la protection des données (RGPD), je souhaite exercer mon droit à obtenir une notification concernant la rectification, l'effacement, ou la limitation du traitement de vos données personnelles conformément à la réglementation en vigueur (*veuillez biffer la mention inutile*).

Je vous remercie de m'adresser la communication de la notification demandée au plus tard dans un délai d'un mois à compter de la réception de ma demande. En cas de non-réponse ou de réponse incomplète, je me réserve la faculté d'adresser une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL) ».

***480.*** Il est proposé ci-après une clause relative au droit d'opposition,

« Dans le cadre de l'exécution du contrat de cloud computing, vous disposez d'un droit d'opposition concernant le traitement des données vous concernant conformément à la réglementation en vigueur. Ce droit d'opposition vous permet de vous opposer à tout moment, auprès de nos Services, à un traitement de vos données personnelles. Vous pouvez exercer votre droit d'opposition en écrivant à : XXXX ou par courriel à l'adresse suivante : XXXX. Nous nous engageons à répondre à vos communications dans un délai maximal de 30 (trente) jours.

Pour exercer votre droit d'opposition au traitement des données personnelles, vous avez la possibilité d'utiliser le formulaire ci-dessous :

*Formulaire pour exercer le droit d'opposition au traitement des données personnelles et à adresser à l'adresse postale suivante xxxx ou par courriel xxxx : (* informations à remplir par le client)*

Nom : *

Prénom : *

Adresse postale : *

Courriel : *

Numéro de téléphone : *

Référence du contrat : *

Madame, Monsieur,

En application de l'article 21 du Règlement général sur la protection des données (RGPD), je souhaite exercer mon droit d'opposition au traitement de mes données personnelles. Je vous remercie de bien vouloir cesser de manière effective, à compter de la réception de ma demande, à tout traitement de mes données personnelles.

Je vous remercie de m'adresser par écrit la confirmation de la cessation du traitement de mes données personnelles au plus tard dans un délai d'un mois à compter de la réception de ma demande. En cas de non-réponse ou de non-cessation du traitement de mes données personnelles, je me réserve la faculté d'adresser une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL) ».

***481.*** Il est proposé ci-après une clause relative au droit à la portabilité,

« Dans le cadre de l'exécution du contrat de cloud computing, vous disposez d'un droit à la portabilité des données vous concernant conformément à la réglementation en vigueur. Ce droit à la portabilité vous permet d'exiger de recevoir, de la part de nos Services, vos données personnelles dans un format adapté et structuré afin de faciliter, le cas échéant, leurs transmissions à un autre responsable du traitement des données. Vous pouvez exercer votre droit à la portabilité des vos données en écrivant à : XXXX ou par courriel à l'adresse suivante : XXXX. Nous nous engageons à répondre à vos communications dans un délai maximal de 30 (trente) jours.

Pour exercer votre droit à la portabilité de vos données personnelles, vous avez la possibilité d'utiliser le formulaire ci-dessous :

*Formulaire pour exercer le droit à la portabilité de vos données personnelles et à adresser à l'adresse postale suivante xxxx ou par courriel xxxx : (* informations à remplir par le client)*

Nom : *

Prénom : *

Adresse postale : *

Courriel : *

Numéro de téléphone : *

Référence du contrat : *

Madame, Monsieur,

En application de l'article 20 du Règlement général sur la protection des données (RGPD), je souhaite exercer mon d'un droit à la portabilité de mes données personnelles. Je vous remercie de bien vouloir me fournir mes données personnelles dans un format adapté (couramment utilisé) et structuré (lisible par machine).

Le cas échéant, je vous remercie de bien vouloir transmettre ces données à caractère personnel directement à mon nouveau responsable du traitement des données, identifié ci-dessous (*veuillez biffer cette mention si elle est inutile*) :

Nom – Prénom ----------

Dénomination sociale ----------

Numéro SIRET ----------

Adresse postale ----------

Adresse électronique ----------
Numéro de téléphone ----------.

Je vous remercie de bien vouloir me transmettre mes données personnelles dans un format adapté et structuré (le cas échéant à mon responsable du traitement identifié ci-dessus), au plus tard dans un délai d'un mois à compter de la réception de ma demande. En cas de non-réponse ou de non-transmission de mes données personnelles, je me réserve la faculté d'adresser une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL) ».

***482.*** Ces propositions de clauses énonçant les prérogatives du droit à l'autodétermination informationnelle, dès lors qu'elles sont intégrées dans le contrat de cloud computing, permettent de contribuer au renforcement de la protection des données personnelles de la personne physique.

***483.*** En définitive, le droit à l'autodétermination informationnelle, spécifique à la matière de la protection des données, constitue un palliatif à l'inadaptation du concept de « propriété » aux données à caractère personnel et s'inscrit dans le cadre d'un renforcement de la protection des données à caractère personnel dès lors que les prérogatives dudit droit sont intégrées par des clauses spécifiques dans le contrat de cloud computing.

# Conclusion chapitre 1

***484. L'inadaptation d'un droit de « propriété » des données.*** Malgré la tentation de vouloir consacrer un droit de propriété des données, il s'avère que le concept de propriété est inadapté à la protection des données dans les contrats de cloud computing. La proposition d'un droit de propriété des données avec une faculté de rétribution au profit des personnes physiques ne convainc pas au regard des exigences du droit français et européen. Il apparaît que l'attribut de la propriété l'*abusus* est difficilement transposable au rapport juridique entre la personne physique et sa donnée. Pour rejeter la thèse d'un droit de propriété, il est rappelé, entre autres, que l'admettre aurait pour incidence d'accepter d'être « dépossédé » des attributs de la personnalité or une telle dépossession porterait atteinte aux droits fondamentaux et contrevient au principe de l'inaliénabilité des droits de la personnalité. En outre, la propriété comprend une dimension purement exclusive dans le rapport à la possession alors que le rapport des personnes à « la donnée » n'est pas caractérisé par une dimension exclusive puisqu'au contraire c'est la circulation et l'usage attendu qui vont créer de la valeur. Dans une approche classique du droit de la propriété, il y a l'idée d'une éventuelle appropriation définitive alors que dans le cadre de la donnée, il est possible de reconnaître des droits personnels concurrents sans pour autant que cela vienne priver la possession ou l'usage de la donnée. Pour toutes ces raisons, cette étude nous amène à considérer que la thèse de la propriété est inadaptée à la protection des données dans les contrats de cloud computing, qu'il est préférable de rejoindre la théorie personnaliste du droit à la protection des données et de développer d'autres droits spécifiques à la protection des données et en particulier le droit à l'autodétermination informationnelle.

***485. La consécration d'un droit à l'autodétermination informationnelle***. En matière de cloud computing, il s'agirait de permettre à la personne concernée d'avoir un droit de contrôle sur ses données à caractère personnel ainsi que la faculté pour elle de déléguer si elle souhaite certaines prérogatives dont elle dispose sur sa donnée sans interférence de la puissance publique ou des acteurs privés. Pour conforter l'effectivité de ce droit à l'autodétermination informationnelle, celui-ci est fondé sur le droit fondamental à la protection des données à caractère personnel. La consécration du droit à l'autodétermination informationnelle par les textes permet de conférer au profit de la personne physique, un droit à la libre disposition de ses données et d'autres prérogatives telles que le droit de consentir à la collecte et au traitement des données, au droit d'information, au droit d'accès, au droit à la limitation du traitement, au droit d'opposition de rectification, d'effacement, au droit à la portabilité des données. En définitive, pour renforcer de manière effective le droit à la protection des données, la déclinaison des droits issus du droit à

l'autodétermination informationnelle doit figurer dans le contenu du contrat de cloud de computing, lesquels ont fait l'objet de propositions rédactionnelles de clauses dans la présente étude.

# Chapitre 2 : Le renforcement par le droit à la réparation

***486.*** ***La mise en œuvre du droit à réparation dans les contrats de cloud computing***. En raison de l'accroissement du nombre des utilisateurs des services cloud et donc d'une hausse potentielle du nombre des victimes d'une atteinte à leur droit à la protection des données à caractère personnel, il apparaît légitime d'établir un cadre juridique qui puisse renforcer le droit à réparation. Ce chapitre est, alors, consacré à l'étude du renforcement de la protection des données personnelles par le droit à la réparation. L'objectif, ici, est de permettre à la personne physique, dans le cadre d'un contrat de cloud computing, d'obtenir une réparation effective de ses préjudices découlant d'une atteinte au droit à la protection des données personnelles.

***487.*** ***La nécessité d'une analyse extraterritoriale de la loi et du contrat.*** Pour que le droit à la réparation des personnes physiques puisse être effectif dans le cadre de l'exécution d'un contrat cloud, il est nécessaire d'appréhender les responsabilités, non seulement dans un contexte européen, mais également international. La notion d'extraterritorialité signifie qu'« État prétend appréhender, à travers son ordre juridique, des éléments situés en dehors de son territoire »[1135]. L'extraterritorialité du droit est un véritable enjeu en matière de protection de données dans les contrats de cloud computing puisque les données se trouvent dans « un nuage » et ne connaissent pas de « frontière étatique » alors que le droit pour pouvoir s'appliquer nécessite la détermination de la territorialité concernée. La réglementation européenne relative à la protection des données à caractère personnel peut être appliquée à des situations qui de prime abord pourraient sembler y échapper[1136] dès lors que la loi[1137] ou le contrat le prévoit[1138].

***488.*** **Plan.** En raison de la perméabilité des frontières physiques dans le cadre de l'exécution d'un contrat de cloud computing, il est envisagé d'étudier l'élargissement des responsabilités dans un contexte européen (section 1) et international (section 2).

---

[1135] Salmon J., Dictionnaire de droit international public, Bruxelles, Bruylant, 2001, p. 211.

[1136] Lorsque par exemple, il est fait application du droit d'un État en vertu du droit international privé : v. considérant 25 du RGPD.

[1137] V. art. 3 paragraphe 3 du RGPD : le RGPD s'applique au traitement lorsque le droit d'un État membre s'applique en vertu du droit international public.

[1138] V. considérant 25 du RGPD : application du RGPD à un responsable du traitement qui n'est pas établi dans l'Union, par exemple qui se trouve auprès de la représentation diplomatique ou consulaire d'un État membre.

## Section 1 : Le renforcement de la protection des données personnelles par un élargissement des responsabilités dans un contexte européen

***489. Le renforcement de la protection des données par un élargissement des responsabilités.*** Afin de rendre effectif le droit à réparation dans le cadre de l'exécution d'un contrat de cloud computing, il est envisagé d'étudier la responsabilité de(s) acteur(s) (prestataire de services cloud, sous-traitant) qui ont porté atteinte au droit à la protection des données personnelles de leurs clients, personnes physiques.

***490. Plan.*** Le renforcement de la protection des données personnelles est envisagé, ici, à travers l'étude d'un élargissement des responsabilités (A) et de la réparation (B).

### A) Le renforcement de la protection des données personnelles par une responsabilité étendue

***491.*** Pour engager la responsabilité du prestataire de services cloud dans le cadre de l'exécution d'un contrat de cloud computing, la personne physique dispose de la faculté d'utiliser les fondements juridiques du droit à la protection des données et du droit à la vie privée. Ces deux droits ont pour nature d'être des droits fondamentaux, mais chacun conserve son autonomie. Le droit fondamental à la protection des données est appréhendé, ici, par le « droit à l'autodétermination informationnelle » tel que déterminé[1139], ci-dessus, dans le chapitre 1 (chap.1, Partie 2, titre 1).

***492. Plan.*** Il convient, donc, d'étudier l'élargissement des responsabilités fondées, d'une part, sur l'atteinte au droit à l'autodétermination informationnelle (1) et d'autre part, sur l'atteinte au droit à la vie privée (2).

#### 1) La responsabilité fondée sur l'atteinte au droit à l'autodétermination informationnelle

***493. Un recours juridictionnel effectif.*** Le droit à l'autodétermination informationnelle tire sa source du droit fondamental à la protection des données à caractère personnel[1140] et fait référence à la déclinaison des droits issus de ce droit fondamental, lesquels sont retranscrits dans

[1139] V. *supra* n° 450 et suivants.

[1140] V. *supra* n° 453.

le RGPD[1141]. Afin de rendre plus effectifs les droits conférés à la personne concernée, ce texte prévoit plusieurs actions judiciaires au profit de cette dernière[1142]. La construction du cadre relatif à la protection des données personnelles s'inscrit dans une dynamique de renforcement du droit à obtenir une réparation[1143] qui se traduit par la mise en place d'une pluralité d'actions en justice[1144]. Ce cadre légal est passé d'une logique de conformité qui nécessitait l'accomplissement préalable de formalités à une logique de responsabilité[1145] qui est fondée, aujourd'hui, sur le risque[1146] et fait naître des obligations à la charge du responsable du traitement. Ce sont les manquements à ses obligations légales qui sont susceptibles d'être mis en cause dans le cadre des actions judiciaires[1147]. Ces actions judiciaires peuvent être regroupées en deux catégories ; celles à caractère individuel et celles à caractère collectif.

***494. Plan***. Dans cette partie, le renforcement de la protection des données personnelles est envisagé à travers l'étude des actions judiciaires à caractère individuel (a) et à caractère collectif (b).

a) Le renforcement de la protection des données personnelles par l'élargissement des actions judiciaires à caractère individuel

***495. L'exercice des actions judiciaires dans les contrats cloud.*** Dans le cadre du RGPD, la personne concernée a le droit de former un recours juridictionnel contre une décision juridiquement contraignante d'une autorité de contrôle qui la concerne[1148] pour certains motifs[1149], contre un responsable du traitement ou un sous-traitant[1150] si elle considère que les droits que lui confère le présent règlement ont été violés du fait d'un traitement de ses données à

[1141] Ibid.

[1142] Danis-Fatôme A., étude, Protection des données - Quelles actions judiciaires en cas de violation du RGPD ? Communication Commerce électronique n° 4, Avril 2018, dossier 18.

[1143] Rochfeld J., Les grandes notions du droit privé : Thémis droit, PUF, 2011, n° 176 s.

[1144] Le RGPD permet une pluralité d'actions en responsabilité contre un responsable de traitement, un co-responsable de traitement ou un sous-traitant mais aussi une action en représentation conjointe et une action de groupe. En ce sens, V. Azar-Baud M.J, De l'inaction aux actions de groupe : nouveaux enjeux : D. 2017, Entretien, p. 152.

[1145] Peyrou S., Le nouveau règlement général européen relatif à la protection des données à caractère personnel : un texte à la hauteur de ses ambitions : RAE-LEA 2016/1, p. 103 s., spéc. p. 106.

[1146] G29, Statement on the role of a risk-based approach in data protection legal frameworks, WP218 30 may 2014.

[1147] Danis-Fatôme A., étude, Protection des données - Quelles actions judiciaires en cas de violation du RGPD ? Communication Commerce électronique n° 4, Avril 2018, dossier 18.

[1148] Considérant 78 du RGPD.

[1149] Exemples : Soit l'autorité de contrôle ne traite pas une réclamation soit n'informe pas la personne concernée, dans un délai de trois mois, de l'état d'avancement ou de l'issue de la réclamation qu'elle a introduite (v.art.78 RGPD).

[1150] V. art.79 du RGPD.

caractère personnel[1151]. Dès lors que le contrat de cloud computing prévoit la collecte ou le traitement des données, les dispositions du RGPD s'appliquent au contrat de cloud computing. Le recours qui intéresse notre étude est, celui exercé par la personne physique contre le responsable du traitement et/ou son sous-traitant. Dans le cadre de l'exécution d'un contrat de cloud computing, le client, personne physique, a la faculté d'exercer un recours juridictionnel[1152] contre le prestataire de services cloud qualifié de responsable du traitement et/ou son sous-traitant dès lors qu'il estime que les droits issus du RGPD ont été enfreints.

***496. L'engagement de la responsabilité du prestataire de services cloud***. Lorsque le RGPD a vocation à s'appliquer au contrat de cloud computing, le respect de ces obligations est à la charge de celui qui est qualifié de responsable du traitement. Il apparaît que « le responsable du traitement est le premier débiteur des obligations mises en place par le RGPD, dans son considérant 78 »[1153] et ces obligations, telles que précédemment étudiées, sont nombreuses[1154]. Le responsable du traitement des données a été défini dans les textes et il n'a pas fallu attendre le RGPD pour disposer d'une définition juridique[1155]. Le responsable du traitement est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement (..) »[1156]. Ce dernier à la charge de veiller au respect de la protection des données personnelles puisque c'est à lui qu'incombe de déterminer les finalités et les moyens du traitement des données, tels que la mise en œuvre de politiques appropriées. Il est précisé que « le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement »[1157]. Il est ajouté au même article que « le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures

---

[1151] La personne concernée exerce son recours soit devant les juridictions de l'État membre dans lequel elle a sa résidence habituelle soit devant les juridictions de l'État membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement. La notion d'établissement fait référence, ici, « à l'exercice effectif et réel d'une activité au moyen d'un dispositif stable » : considérant 22 du RGPD, v. également, article 4, 16) du RGPD qui définit la notion « d'établissement principal ».

[1152] V. art.79 du RGPD.

[1153] Danis-Fatôme A., étude, Protection des données - Quelles actions judiciaires en cas de violation du RGPD ? Communication Commerce électronique n° 4, Avril 2018, dossier 18.

[1154] Metallinos V. N. et Perray R., Le périmètre du RGPD : Comm. com. électr. 2018, dossier 4.

[1155] En 1995, nous disposions déjà d'une définition à l'article 2 d) de la Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données et à la libre circulation des données qui définit le responsable de traitement des données comme « toute personne qui seule ou conjointement avec d'autres détermine les finalités et les moyens du traitement de données à caractère personnel ».

[1156] V. art. 4 du RGPD.

[1157] V. art. 24 du RGPD.

techniques et organisationnelles appropriées »[1158]. Le critère, ici, permettant de retenir la qualification de responsable du traitement, est l'autonomie de « l'entité » à dicter les finalités et les moyens du traitement des données. Le prestataire de services cloud (personne morale incarnée par le représentant légal, personne physique) sera qualifié de responsable du traitement dès lors qu'il détermine les objectifs et les moyens pour collecter et traiter les données personnelles de son client. Dès lors que la qualification de « responsable du traitement » est retenue, elle entraine une responsabilité[1159]. Il incombe au responsable du traitement de respecter les principes de protection des données à caractère personnel. La contravention à ces obligations légales ouvre au profit du client, personne physique, victime d'un dommage, un recours juridictionnel contre son prestataire de services agissant en qualité de responsable du traitement[1160] afin d'obtenir la réparation d'un dommage moral et matériel[1161]. Outre la responsabilité du prestataire de services cloud agissant en qualité de responsable du traitement, il est également possible d'engager sous certaines conditions la responsabilité de son sous-traitant.

***497. La définition du sous-traitant par la réglementation protectrice des données à caractère personnel.*** À l'instar du « responsable du traitement des données », le « sous-traitant » a été défini par la directive de 1995 comme étant « la personne qui traite des données à caractère personnel pour le compte du responsable de traitement des données »[1162]. Par la suite, le RGPD a précisé que le sous-traitant est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »[1163]. La CNIL définit le sous-traitant comme « celui qui traite les informations personnelles pour le compte du responsable du traitement de données selon ses instructions et qui pourrait faire l'objet d'une présomption légale pour le prestataire agissant pour le compte et sur les instructions du client afin de simplifier les relations juridiques entre les opérateurs »[1164]. Il ressort de ces éléments de définitions que le «sous-traitant» est celui qui va exécuter, dans le cadre d'un contrat, les directives d'un client «donneur d'ordre». Dans le cadre d'une sous-traitance de prestations de services cloud, le client donneur d'ordre est le prestataire

[1158] V. art. 25 du RGPD.

[1159] V. art. 5 et 7 du RGPD.

[1160] Danis-Fatôme A., étude, Protection des données - Quelles actions judiciaires en cas de violation du RGPD ? Communication Commerce électronique n° 4, Avril 2018, dossier 18.

[1161] V. art. 82 du RGPD. V. également, Danis-Fatôme A., étude, Protection des données - Quelles actions judiciaires en cas de violation du RGPD ? Communication Commerce électronique n° 4, Avril 2018, dossier 18.

[1162] V. art. 2, e) Directive de 1995.

[1163] V. art. 4 du RGPD.

[1164] Définition de sous-traitant par la CNIL : https://www.cnil.fr/.

de services principal. Dans cette configuration, c'est par le biais d'un faisceau d'indicateurs qu'il sera possible de déterminer si le prestataire en cause doit être qualifié de « responsable du traitement des données » ou de « sous-traitant »[1165].

***498. L'identification de l'opération de sous-traitance dans le cadre d'une prestation de cloud computing***. Dans les contrats de cloud computing, il est fréquent que la prestation de services de cloud computing soit exécutée par un tiers au contrat principal dans le cadre d'un contrat de sous-traitance. C'est l'article 1er de la loi du 31 décembre 1975[1166] qui définit la sous-traitance de marché comme étant « l'opération par laquelle un "entrepreneur" confie par "un sous-traité", et sous sa responsabilité, à une autre personne appelée "sous-traitant" l'exécution de tout ou partie du contrat d'entreprise ou d'une partie du marché "public" conclue avec le maître d'ouvrage »[1167]. En application de cette loi, tous types de prestations peuvent faire l'objet d'une sous-traitance de marché à partir du moment où la prestation s'inscrit dans le cadre d'un contrat d'entreprise. La troisième chambre civile de la Cour de cassation dans son arrêt du 18 avril 1972[1168] a considéré au visa de la loi de 1975 que la sous-traitance de marché est « le montage contractuel en vertu duquel un entrepreneur principal fait exécuter tout ou partie du contrat d'entreprise dont il est titulaire par un autre entrepreneur »[1169].

***499. Le montage contractuel de la sous-traitance dans le cadre d'une opération de cloud computing.*** Dans le cadre d'un contrat de cloud computing, le prestataire principal pourra recourir à une sous-traitance pour l'exécution de la prestation de services de cloud computing. Le montage contractuel est le suivant, un client (personne physique ou morale) fait appel à une prestataire de services de cloud computing, appelé « prestataire principal », lequel va faire exécuter toute ou partie de la prestation de services cloud par une autre personne morale « le sous-traitant ». Dans cette configuration, la question se pose de savoir qui est le responsable en cas d'atteinte à la protection des données. Il est intéressant de rappeler que dans le cadre d'une sous-traitance d'une prestation de services, nous sommes en présence de deux contrats

---

[1165] Illustration du faisceau d'indices : La CNIL considère que « le niveau élevé de précision des instructions préalables données par le responsable de traitement, le prestataire dispose de peu de liberté et rend compte régulièrement à son client de l'exécution de ses prestations, si le prestataire ne se présente pas en son nom et ne réutilise pas les données pour son propre compte » ; lorsque le prestataire dispose d'une expertise dans son domaine et l'utilise pour décider des moyens à mettre en place dans le cadre de la réalisation des prestations, il est qualifié de « responsable du traitement des données » : https://www.cnil.fr/.

[1166] Article 1er de la loi n° 75-1334 du 31 décembre 1975 relative à la sous-traitance : « Au sens de la présente loi, la sous-traitance est l'opération par laquelle un entrepreneur confie par un sous-traité, et sous sa responsabilité, à une autre personne appelée sous-traitant l'exécution de tout ou partie du contrat d'entreprise ou d'une partie du marché public conclu avec le maître de l'ouvrage ».

[1167] Traité de droit civil du numérique., Gaudrat Ph., Sardain F., édition Larcier 2015, Tome 2 Droit des obligations, p. 159.

[1168] Cass. 3e civ., 18 avril 1972, pourvoi n°71-10.660, Bull.civ.III, n°237.

[1169] Traité de droit civil du numérique. Tome 2 Droit des obligations Gaudrat Ph., Sardain F., édition Larcier 2015 : page 160, paragraphe 298.

enchaînés ; le premier entre le client (personne physique ou morale) et le prestataire de services principal puis entre le prestataire de services principal et le sous-traitant. L'existence de deux contrats enchaînés, dans l'opération de sous-traitance, pose le problème de la nature juridique de l'action en responsabilité du client contre le sous-traitant.

***500. La nature des actions en responsabilité contre le prestataire de services et son sous-traitant***. La responsabilité dans le cadre d'une opération de sous-traitance soulève des interrogations particulières et notamment celle relative au choix du régime de la responsabilité applicable dans les rapports avec l'entrepreneur principal et dans les rapports avec le sous-traitant. En droit civil, il existe deux types de responsabilités, la responsabilité contractuelle [1170] et la responsabilité délictuelle[1171]. La première étant définie comme étant la responsabilité qui est encourue par une partie à un contrat ayant manqué à une de ses obligations contractuelles et la seconde est la responsabilité « de toute personne qui, sans contrat, crée un dommage à autrui par sa faute, contrevenant ainsi à une obligation légale générale et implicite de diligence et de précaution dans le comportement »[1172]. Ces définitions permettent d'éclairer sur l'action à privilégier dans le cadre de la sous-traitance d'une prestation de services de cloud computing. En l'espèce, le client (personne physique ou morale) a passé un contrat avec le prestataire principal et n'a, en revanche, aucun lien contractuel avec le sous-traitant. Par conséquent, il est question de distinguer les actions en fonction que le client souhaite agir contre le prestataire principal ou contre le sous-traitant. Concernant les rapports entre le client et le prestataire principal de services de cloud computing, le régime de la responsabilité est essentiellement contractuel, car il est lié par un contrat et tout manquement ou mauvaise exécution engage sa responsabilité avec une distinction selon qu'il s'agit d'une obligation de résultats ou de moyens[1173]. Concernant les rapports entre le client et le sous-traitant de services de cloud computing, le régime applicable est celui de la responsabilité délictuelle. Il n'existe aucun contrat entre le client et le sous-traitant ayant pour mission d'exécuter la prestation de services de cloud computing. Il s'agira, alors, du régime de la responsabilité délictuelle puisque le client est un tiers au contrat conclu entre le prestataire principal et le sous-traitant. Cette position a été

[1170] L'action en responsabilité contractuelle est fondée sur les articles 1103 ; 1193 ou 1194 du Code civil (ancien article 1134).

[1171] Le principe est que toute personne qui cause un préjudice à autrui soit par sa faute, soit par sa négligence en doit réparation. L'article 1240 du Code civil (ancien article 1382) : « Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer » ; L'article 1241 du Code civil (ancien article 1383) : « Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence ». Au succès de cette action, il faudra apporter la preuve d'une faute, d'un préjudice et un lien de causalité.

[1172] Traité de droit civil du numérique. Tome 2 Droit des obligations. Gaudrat Ph., Sardain F., édition Larcier 2015 : page 165, paragraphe 313.

[1173] En application des articles 1103, 1193 ou 1194 du Code civil (ancien article 1134).

affirmée dans l'arrêt BESSE de la Cour de cassation statuant en assemblée plénière le 12 juillet 1991[1174].

***501.*** Outre ces règles issues du droit commun, en matière de protection des données, le RGPD encadre l'engagement de la responsabilité du responsable du traitement et de son sous-traitant.

***502. L'engagement de la responsabilité du sous-traitant en matière de protection des données personnelles.*** En matière de cloud computing, la relation entre le sous-traitant et le prestataire de services cloud est formalisée par la conclusion d'un contrat de sous-traitance, lequel doit revêtir certaines mentions telles que l'objet, la durée du traitement, la nature et la finalité du traitement, les types de données à caractère personnel et les catégories de personnes concernées ainsi que les obligations et les droits du responsable du traitement[1175]. Dans le cadre d'une sous-traitance d'une prestation de services cloud, la question se pose de savoir envers qui le client final, personne physique, peut engager une action en cas de préjudices découlant d'une atteinte à son droit à la protection des données. Pour identifier le responsable du dommage, la personne physique doit se référer au contrat cloud principal signé avec son prestataire de services cloud (responsable du traitement). Si le contrat de cloud computing précise que le sous-traitant n'agit que sur instruction du responsable du traitement des données, dans ce cas, la responsabilité du sous-traitant ne pourra pas être engagée puisqu'il ne détermine pas les finalités et les moyens du traitement des données[1176]. Il en résulte que c'est le prestataire de services cloud qui doit répondre de sa responsabilité et non le « sous-traitant » qui lui ne répond que de ses engagements contractuels prévus au contrat de sous-traitance.

***503. Le renforcement de la protection des données par un élargissement de la responsabilité.*** Le droit à réparation est renforcé dans le RGPD avec la possibilité offerte à la personne physique d'engager la responsabilité conjointe du responsable du traitement et du sous-traitant[1177] dès lors que « deux responsables ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement »[1178]. Il est précisé, à

---

[1174] Cass, Ass. Plén. du 12 juillet 1991, pouvoir n° 90-13.602, Bull. Ass. plén. n° 5, Besse c/ Protois BIF : « Alors que le maître de l'ouvrage ne dispose contre le sous-traitant, avec lequel il n'a aucun lien contractuel, que d'une action de nature quasi délictuelle soumise, avant l'entrée en vigueur de la loi du 5 juillet 1985, à la prescription trentenaire du droit commun ; que la cour d'appel ne pouvait estimer que M. Y..., maître de l'ouvrage, ne disposait contre M. Z..., sous-traitant, que d'une action de nature nécessairement contractuelle soumise au délai de prescription décennale, nonobstant le fait que M. Y... n'avait aucun lien contractuel avec M. Z... ; qu'en statuant ainsi la cour d'appel a violé les articles 1165, 1792 et 2270 du Code civil ».

[1175] V. art. 28 du RGPD.

[1176] V. art. 24 du RGPD.

[1177] Danis-Fatôme A., étude, Protection des données - Quelles actions judiciaires en cas de violation du RGPD ? Communication Commerce électronique n° 4, Avril 2018, dossier 18.

[1178] V. art. 26 du RGPD.

ce titre, que « chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage causé dans sa totalité afin de garantir à la personne concernée une réparation effective »[1179]. Cette responsabilité conjointe permet de garantir et de renforcer les droits de la personne concernée et notamment le droit à la réparation[1180]. Cette faculté d'engager une action conjointe à l'égard des deux responsables ne prive pas la personne physique d'agir à l'égard de et contre chacun des responsables du traitement[1181].

***504.*** Pour renforcer davantage l'effectivité des droits de la personne concernée et contrairement à ce qui était prévu par la directive du 24 octobre 1995, le RGPD a mis en place un régime de responsabilité autonome contre le sous-traitant[1182] accompagné d'obligations qui lui sont spécifiques[1183] . Le RGPD désigne tant le responsable du traitement que le sous-traitant comme débiteurs des obligations[1184]. C'est l'article 28 du RGPD qui énonce les obligations dévolues au sous-traitant[1185]. Il incombe au sous-traitant, au même titre que le responsable du traitement, de procéder à la réparation de tout dommage résultant d'un traitement réalisé en contravention aux prescriptions du règlement[1186]. La personne concernée, par ce dommage, peut décider d'exercer son action en responsabilité de manière autonome à l'encontre du sous-traitant que du responsable du traitement[1187]. Ce texte a été considéré, par la doctrine, comme sonnant « la fin de l'« impunité »[1188] du sous-traitant »[1189]. Les critères pour apprécier la responsabilité du responsable du traitement ou du sous-traitant ne sont pas identiques. Il est précisé que « tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du présent règlement » alors qu'« un sous-traitant n'est

---

[1179] V. art. 82, al. 5 du RGPD.

[1180] En présence d'une responsabilité conjointe, le RGPD règle la question de l'obligation à la dette et de la contribution à la dette pesant sur le(s) responsable(s) du traitement et le(s) sous-traitant(s) : V. considérant 146 du RGPD.

[1181] V. art. 26, al. 3 du RGPD.

[1182] Metallinos N., Les critères de la qualification des acteurs : Comm. com. électr. 2018, dossier 8.

[1183] Banck A., GDPR et sous-traitance : un nouveau devoir de conseil ? : Dalloz IP/IT, 2017, p. 36.

[1184] V. cons.146 du RGPD : le texte a pour objet « d'offrir aux personnes physiques de tous les États membres un même niveau de droits opposables et d'obligations et de responsabilités pour les responsables du traitement et les sous-traitants ».

[1185] Ces obligations se rattachent aux conditions prévues dans le RGPD concernant la collecte et le traitement des données.

[1186] Danis-Fatôme A., étude, Protection des données - Quelles actions judiciaires en cas de violation du RGPD ? Communication Commerce électronique n° 4, Avril 2018, dossier 18.

[1187] V. art. 79 du RGPD. « Contrairement à ce que prévoyait l'article 23 de la directive de 1995 ( Dir. 95/46/CE, 24 oct. 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données) et l'article 34 de la loi du 6 janvier 1978 (L. n° 78-17, 6 janv. 1978 , relative à l'informatique, aux fichiers et aux libertés) » : Danis-Fatôme A., étude, Protection des données - Quelles actions judiciaires en cas de violation du RGPD ?, Communication Commerce électronique n° 4, Avril 2018, dossier 18.

[1188] Metallinos N., Introduction d'une action de groupe en matière de violation de la loi Informatique et Libertés : Comm. com. électr. 2016, comm. 95, spéc. p. 40.

[1189] Danis-Fatôme A., étude, Protection des données - Quelles actions judiciaires en cas de violation du RGPD ? Communication Commerce électronique n° 4, Avril 2018, dossier 18.

tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par le présent règlement qui incombent spécifiquement aux sous-traitants ou qu'il a agi en dehors des instructions licites du responsable du traitement ou contrairement à celles-ci »[1190].

***505.*** Il en résulte de cette analyse que la protection des données à caractère personnel est renforcée par la possibilité, pour la personne physique, d'engager la responsabilité de son prestataire de services cloud (en sa qualité de responsable du traitement) ou de son sous-traitant (responsabilité autonome) ou bien d'engager la responsabilité conjointe (du prestataire de services cloud et du sous-traitant).

***506. Une inversion de la charge de la preuve au profit de la personne physique***. Pour renforcer le droit à réparation des personnes physiques dans le cadre d'une action judiciaire en responsabilité, le RGPD procède à une inversion de la charge de la preuve. Le principe de la charge de la preuve est énoncé à l'article 24 du RGPD qui dispose que « le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement ».Ce texte instaure, donc, « une inversion de la charge de la preuve »[1191] par rapport au régime du droit commun de la responsabilité civile qui met à la charge du demandeur à l'action en responsabilité délictuelle d'apporter la preuve de trois conditions : la faute, le préjudice et le lien de causalité. L'inversion de la charge de preuve, ici, profite au client, personne physique ayant subi un préjudice dans le cadre de l'exécution de son contrat cloud puisqu'il n'a pas à apporter la preuve que le prestataire de services cloud a contrevenu à son droit à la protection des données personnelles. Au contraire, il incombe au prestataire de services cloud d'apporter la preuve qu'il s'est conformé aux prescriptions du RGPD. En raison de cette inversion de la charge de la preuve, il est plus opportun d'engager cette action spéciale en responsabilité que l'action exercée sur le fondement du droit commun de la responsabilité civile (articles 1240 et 1241 du code civil)[1192]. Cette inversion de la charge de la preuve permet, ainsi, de renforcer l'effectivité des droits de la personne concernée pour la protection de ses données personnelles et en particulier du droit à réparation.

---

[1190] V. art. 82 § 2 du RGPD.

[1191] Danis-Fatôme A., étude, Protection des données - Quelles actions judiciaires en cas de violation du RGPD ? Communication Commerce électronique n° 4, Avril 2018, dossier 18.

[1192] Danis-Fatôme A., étude, Protection des données - Quelles actions judiciaires en cas de violation du RGPD ? Communication Commerce électronique n° 4, Avril 2018, dossier 18. Egalement, v. not. Traullé J., L'éviction de l'article 1382 du Code civil en matière extracontractuelle : LGDJ, 2007.

***507. Le non-cumul des responsabilités délictuelle et contractuelle***. Le prestataire de services cloud, en qualité de responsable du traitement, engage sa responsabilité extracontractuelle en cas de non-conformité aux prescriptions du RGPD[1193]. En l'espèce, il s'agit de retenir la commission d'une faute du prestataire de services qui à sa source dans le manquement de « devoir extracontractuel »[1194]. En l'espèce, il s'agit d'une contravention à des obligations légales. Il en résulte que la responsabilité, ainsi, engagée est de nature délictuelle puisque le fondement juridique est légal. Sur la distinction de la nature de l'action judiciaire (délictuelle, contractuelle), certains auteurs considèrent que « les obligations contractuelles n'ont pas en principe pour vocation d'imposer des règles de conduite »[1195]. En revanche, il est toujours possible de renforcer ces obligations légales en les inscrivant dans le contrat cloud par des clauses spécifiques. Dans un tel cas de figure, la violation des règles contractuelles entrainera la responsabilité contractuelle du prestataire de services cloud. Si les demandes de réparation du préjudice portent sur le même objet, alors, le client, personne physique, devra opter pour l'une des actions et non les deux. En effet, « le principe est que les responsabilités contractuelle et délictuelle ne peuvent se cumuler dès lors que les demandes de réparation du préjudice subi portent sur le même objet »[1196].

***508.*** Ce droit à un recours juridictionnel effectif permet, par son inscription expresse dans le RGPD, de lui conférer une véritable assise et donc de contribuer au renforcement de la protection des données des personnes physiques dans le cadre d'un contrat de cloud computing. En outre, l'action individuelle en responsabilité exercée à l'encontre du responsable du traitement ou le sous-traitant se trouve complété par des actions à caractère collectif[1197].

b) Le renforcement de la protection des données par l'élargissement des actions judiciaires à caractère collectif

***509. L'engagement de la responsabilité du prestataire de services cloud et/ou son sous-traitant dans le cadre d'une action de groupe.*** L'affirmation des droits d'agirse traduit aussi par la faculté réservée aux personnes physiques du droit d'introduire une action de groupe appelée aussi « recours collectif » permettant à plusieurs personnes, ayant subi le même préjudice, de se regrouper pour exercer une action juridictionnelle contre l'auteur du dommage. L'action de

[1193] V. art. 82 § 2 du RGPD.

[1194] Viney G., Jourdain P. et Carval S., Traité de droit civil, Les conditions de la responsabilité : LGDG, 4e éd., 2013, n° 447.

[1195] Ibid.

[1196] Cass. com., 4 décembre 2019, pourvoi n° 17-20.032.

[1197] Amrani-Mekki S., Les notions de pluralité de parties, in La pluralité de parties, 3es rencontres de procédure civile, (dir.) L. Cadiet et D. Loriferne : IRJS 2013, p. 21 s.

groupe en matière de protection des données personnelles est prévue à l'article 80-2 du RGPD[1198] qui énonce que : « les États membres peuvent prévoir que tout organisme, organisation ou association (..) indépendamment de tout mandat confié à une personne concernée, a, dans l'État membre en question, le droit d'introduire une réclamation auprès de l'autorité de contrôle qui est compétente en vertu de l'article 77, et d'exercer les droits visés aux articles 78 et 79 s'il considère que les droits d'une personne concernée prévus dans le présent règlement ont été violés du fait du traitement ». Cette disposition européenne est perçue, par certains, comme étant « une invitation faite aux États membres à créer une action de groupe spéciale en matière de protection des données personnelles »[1199]. Sur ce point, la France est devancière puisque la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle (art. 62 à 84)[1200] a étendu l'action de groupe créée en 2014 en droit de la consommation[1201], à la protection des données personnelles en l'intégrant dans la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[1202]. Il est spécifié que « lorsque plusieurs personnes physiques placées dans une situation similaire subissent un dommage ayant pour cause commune un manquement de même nature aux dispositions de la présente loi par un responsable de traitement de données à caractère personnel ou un sous-traitant, une action de groupe peut être exercée devant la juridiction civile ou la juridiction administrative compétente »[1203]. Il s'agit de la consécration de l'action de groupe « spéciale »[1204] réservée à la protection des données personnelles. Le droit français se trouvait, alors, déjà en conformité avec l'article 80, paragraphes 1 et 2, du RGPD concernant l'intégration de l'action de groupe[1205]. En revanche, l'action de groupe initialement introduite en droit français[1206] n'avait que pour objet de faire cesser le manquement constaté aux prescriptions légales du droit à la protection des données personnelles et non à réparer le préjudice subi[1207].

---

[1198] Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

[1199] Danis-Fatôme A., étude, Protection des données - Quelles actions judiciaires en cas de violation du RGPD ? Communication Commerce électronique n° 4, Avril 2018, dossier 18.

[1200] Loi n°2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle, Action de groupe (articles 62 à 84).

[1201] Loi n° 2014-344 du 17 mars 2014, relative à la consommation, dite loi « Hamon », art. 1er et 2 : il s'agit d'une action de groupe (ou procédure de poursuite collective) qui permet à des consommateurs, victimes d'un même préjudice de la part d'un professionnel, de se regrouper et d'agir en justice.

[1202] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Anc. art. 43 ter, aujourd'hui art. 37).

[1203] V. art. 37 L. n° 78-17, 6 janv. 1978.

[1204] Dans le sens « spécifique » à la protection des données personnelles, contrairement à l'action de groupe dite « générale » ouverte aux consommateurs en vertu des art. 1 et 2 de la loi n° 2014-344 du 17 mars 2014, relative à la consommation, dite loi « Hamon » . Ici, il est mis en application le principe selon lequel « le spécial exclut le général (specilia generalibus derogant) ».

[1205] Danis-Fatôme A., étude, Protection des données - Quelles actions judiciaires en cas de violation du RGPD ? Communication Commerce électronique n° 4, Avril 2018, dossier 18.

[1206] Loi n°2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle, Action de groupe (articles 62 à 84).

[1207] Féral-Schuhl Ch, Chapitre 112 - Des droits de la personne renforcés, 112.163. Recours collectif, Praxis Cyberdroit, 2020-2021.

***510.*** Concernant l'objet de l'action de groupe prévu par le RGPD[1208], il a été laissé une certaine latitude aux États en particulier concernant la faculté d'une réparation du préjudice. Sur ce point, la doctrine considérait que la voie de l'action de groupe serait d'une plus grande efficacité s'il est adjoint à la cessation de l'illicite[1209], la possibilité d'obtenir au profit de la personne concernée une réparation du préjudice. Cette position fut partagée par le Conseil national du numérique (CNNum)[1210] et la CNIL[1211] . Alors que pour le Conseil d'État, l'action de groupe devait se cantonner à la cessation de la violation des prescriptions légales et non à l'obtention de la réparation du préjudice des personnes concernées[1212]. Malgré cette divergence de positions, l'article 37 de la loi du 6 janvier 1978 modifié par l'ordonnance du 12 décembre 2018 prévoit ces deux possibilités,[1213] lesquelles sont reprises également à l'article 62 de la loi du 18 novembre 2016[1214]. L'objet de cette action de groupe est, donc, d'obtenir la cessation d'une atteinte au droit à la protection des données à caractère personnel ainsi que d'engager la responsabilité de la personne ayant causé le dommage afin d'obtenir une réparation du préjudice dès lors que les faits se sont produits après l'entrée en vigueur du RGPD, soit le 25 mai 2018[1215]. Cette intégration dans la loi contribue, ainsi, à renforcer le droit à la protection des données personnelles des personnes physiques.

***511.*** Concernant les effets de l'action de groupe, il y a une distinction à savoir si le manquement a eu lieu avant ou après le 25 mai 2018 (date d'entrée en vigueur du RGPD)[1216]. Avant le 25 mai 2018, le juge a la faculté d'ordonner la cessation de la violation des données personnelles. Après le 25 mai 2018, outre la possibilité d'ordonner la cessation de la violation des données

---

[1208] V. art. 80 du RGPD.

[1209] Bloch C., La cessation de l'illicite, Recherche sur une fonction méconnue de la responsabilité civile extracontractuelle : Dalloz, 2008.

[1210] Rapport « Ambition numérique » remis par le CNNum, le 18 juin 2015, au Premier ministre, proposition n° 5, p. 57.

[1211] CNIL, délib. n° 2017-299, 30 nov. 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978, p. 29.

[1212] CE, Étude annuelle 2014, Le numérique et les droits fondamentaux : Doc. fr. 2014, p. 284.

[1213] V. art. 37- III, L. n° 78-17, 6 janv. 1978 (modifié par l'ordonnance n°2018-1125 du 12 décembre 2018 - art. 1.) - « Cette action peut être exercée en vue soit de faire cesser le manquement mentionné au II, soit d'engager la responsabilité de la personne ayant causé le dommage afin d'obtenir la réparation des préjudices matériels et moraux subis, soit de ces deux fins. Toutefois, la responsabilité de la personne ayant causé le dommage ne peut être engagée que si le fait générateur du dommage est postérieur au 24 mai 2018 ».

[1214] V. art. 62, L. n° 2016-1547, du 18 nov. 2016 : « Lorsque plusieurs personnes placées dans une situation similaire subissent un dommage causé par une même personne, ayant pour cause commune un manquement de même nature à ses obligations légales ou contractuelles, une action de groupe peut être exercée en justice au vu des cas individuels présentés par le demandeur. Cette action peut être exercée en vue soit de la cessation du manquement mentionné au premier alinéa, soit de l'engagement de la responsabilité de la personne ayant causé le dommage afin d'obtenir la réparation des préjudices subis, soit de ces deux fins ».

[1215] Loi n°2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle, Action de groupe (articles 62 à 84). Egalement, v. art. 37 L. n° 78-17, 6 janv. 1978.

[1216] V. art. 37- III, L. n° 78-17, 6 janv. 1978 (modifié par l'ordonnance n°2018-1125 du 12 décembre 2018 - art. 1.)

personnelles[1217], le juge a la faculté d'ordonner l'indemnisation des personnes rattachées à l'action de groupe (chaque personne est indemnisée individuellement) portant sur un préjudice matériel (exemple, une perte financière à la suite d'un vol commis à cause de la divulgation de vos données personnelles) ou moral (exemple, la réputation de la personne physique est atteinte à cause de la publication de données personnelles)[1218]. Concernant l'exercice de l'action de groupe, il convient que deux personnes au minimum estiment avoir subi un préjudice identique résultant du même manquement du prestataire de services[1219]. Ensuite, c'est l'association ou tout organisme légalement habilité qui engage l'action de groupe au nom de toutes les personnes concernées[1220]. La personne concernée dispose la faculté de mandater à cet effet l'association ou l'organisme habilité pour exercer un recours contre l'auteur du dommage[1221], en l'espèce, le prestataire de services et/ou son sous-traitant.

***512.*** Dans ces conditions, l'introduction de cette action de groupe dans le RGPD et dans la loi de 1978 a eu pour objectif de contribuer au renforcement de la protection des données à caractère personnel. En effet, la personne physique délègue sa défense à une association spécialisée pour entreprendre une action judiciaire chargée de représenter l'intérêt des personnes concernées et de demander la réparation au profit de ces mêmes personnes. Les personnes physiques, qui subissent un dommage commun résultant d'une violation aux prescriptions légales de la protection des données à caractère personnel, pourront, donc, se faire représenter dans le cadre d'une action de groupe. Il s'agit de l'application d'un droit à la représentation prévu à l'article 80 du RGPD. Le droit à la représentation est fondamental pour que des professionnels spécialisés dans les problématiques de protection des données à caractère personnel puissent engager les actions adéquates en fonction de l'atteinte et assurer une défense effective. Le droit à la représentation figure, alors, parmi les droits permettant un renforcement de la protection des données à caractère personnel des personnes physiques.

***513.*** Outre la possibilité pour la personne physique d'obtenir une réparation dans le cadre d'une action judiciaire fondée sur l'atteinte au droit à l'autodétermination informationnelle (droit à la

[1217] Concernant la condamnation du prestataire de services cloud à la cessation du manquement aux obligations légales, le juge a la faculté en application de l'article 826-6 du code de procédure civile de désigner un tiers chargé de suivre « les mesures destinées à faire cesser le manquement ».

[1218] V. art. 37 L. n° 78-17, 6 janv. 1978

[1219] Ibid.

[1220] Il s'agit des associations régulièrement déclarées depuis cinq ans au moins ayant dans leur objet statutaire la protection de la vie privée ou la protection des données à caractère personnel ; des associations de défense des consommateurs représentatives au niveau national et agréées lorsque le traitement de données à caractère personnel affecte des consommateurs ; des organisations syndicales de salariés ou de fonctionnaires représentatives : v. Art. 37, L. n° 78-17, 6 janv. 1978).

[1221] Féral-Schuhl Ch, Chapitre 112 - Des droits de la personne renforcés, 112.163. Recours collectif, Praxis Cyberdroit, 2020-2021.

protection des données personnelles), elle peut également agir sur le fondement du droit à la vie privée.

**2) La responsabilité fondée sur l'atteinte au droit à la vie privée**

***514. La protection des données personnelles par le droit fondamental à la vie privée***[1222]***.*** L'enjeu, en matière de cloud computing, est de déterminer si les personnes physiques peuvent se prévaloir d'un droit autonome fondé sur le droit à la vie privée pour protéger les données personnelles dans le cadre d'un contrat cloud. Autrement dit, est-ce que la seule violation des principes découlant du droit à la protection des données porterait atteinte à leur droit à la vie privée, en l'absence même de tout préjudice[1223]. Pour répondre, à cette question, il faut, en amont, procéder à une analyse fonctionnelle de la notion de réparation en matière de protection des données à caractère personnel. La méthode fonctionnelle est celle retenue en droit comparé pour appréhender « une question commune à plusieurs ordres juridiques »[1224]. Pour cela, il faut surmonter la première difficulté tenant à « l'inapplicabilité des concepts juridiques existants aux problèmes nouveaux posés par le traitement de données personnelles »[1225]. Juridiquement, l'application du droit à la vie privée et le droit à la protection des données sont des concepts autonomes. Selon le rapport d'information du Sénat, la protection des données personnelles devrait être conçue « comme un droit autonome et spécifique dont la reconnaissance devrait être élevée au niveau constitutionnel »[1226]. À l'instar des autres droits fondamentaux, le droit à la vie privée bénéficie d'une protection juridique se traduisant par la possibilité d'intenter une action judiciaire.

***515. L'exercice d'une action judiciaire sur le fondement du droit à la vie privée.*** Pour savoir si une action peut être engagée sur le fondement du droit à la vie privée, il convient au préalable d'identifier si une atteinte au droit à la vie est réalisée par le prestataire de services de cloud computing.Tel que nous l'avons indiqué précédemment, les données à caractère personnel constituent une catégorie de données plus vaste que celle relative aux données relatives à la vie

[1222] V. *supra* n° 95 et suivants.

[1223] Lassalle M., étude, Droit à l'autodétermination informationnelle - La réparation des atteintes au droit à l'autodétermination informationnelle, Communication Commerce électronique n° 2, Février 2021, étude 4 ; V. « Comme l'a justement formulé Hakim Gali s'agissant du droit français : « en cas de violation d'un droit de la personnalité, le préjudice moral peut être de deux ordres : celui inhérent à l'atteinte et ceux, éventuels, qui résultent de celle-ci » » : Gali H., Le préjudice moral en droit de la responsabilité civile, thèse, Université Paris-Saclay, 2019, 555 p., p. 241-242.

[1224] Ibid.

[1225] Ibid.

[1226] Sénat, Rapport d'information relatif au respect de la vie privée à l'heure des mémoires numériques, no 441/2009, p. 111.

privée[1227]. Le concept de vie privée regroupe tout ce qui se rapporte à la vie privée et à l'intimité d'une personne. Dans le cadre du droit à la vie privée, ces informations personnelles ont été définies comme « ces faits, communication ou opinions qui concernent l'individu et dont il serait raisonnable d'attendre de lui qu'il les considère comme intimes ou sensibles, et qu'il veuille en conséquence en empêcher ou au moins en restreindre leurs collecte, usage ou circulation »[1228]. En application de la jurisprudence nationale et européenne, le droit à la vie privée recouvre plusieurs hypothèses et protège différents éléments, tels que l'identité de la personne, l'intimité de la personne regroupant la nudité, la vie conjugale (les fiançailles, le mariage, les divorces, la maternité, l'esthétique, la santé de la personne, les souvenirs de la personne, les convictions religieuses, politiques, philosophiques, le patrimoine)[1229]. Il apparaît que « la vie privée est en effet traditionnellement plutôt considérée comme une protection pour les informations confidentielles, secrètes, et ne s'appliquerait donc pas naturellement aux cas dans lesquels ce sont des traitements et non des divulgations publiques qui sont en cause »[1230]. Il faut ainsi comprendre que l'atteinte au droit à la vie privée résulterait d'une divulgation des informations rattachées à l'intimité de la personne et non spécifiquement d'un manquement aux règles relatives au traitement des données qui concernent l'ensemble des données à caractère personnel. Cette différence peut paraître subtile pour une personne lambda, mais a une importance dans le cadre d'une action judiciaire.

***516. La mise en œuvre de l'action fondée sur une atteinte au droit à la vie privée***. Bien que le droit à la vie privée dispose d'un champ moins large que le droit fondamental à la protection des données à caractère personnel[1231], il peut être utilisé à titre de fondement juridique dans le cadre d'une action en responsabilité à l'encontre du prestataire de services cloud. Le fondement du droit à la vie privée est utilisé pour protéger certaines informations relevant uniquement de la vie privée et non toutes les informations personnelles. Lorsqu'il sera envisagé d'agir sur le fondement de l'atteinte au droit à la vie privée dans le cadre de l'exécution d'un contrat de cloud computing, il faudra en amont déterminer que la donnée concernée soit effectivement une information relevant de la vie privée. Une atteinte à la vie privée de la personne physique peut être constituée dans le cadre d'un traitement et/ou d'une collecte non autorisée des données à

[1227] Lepage A., La protection contre le numérique : les données personnelles à l'aune de la loi pour une République numérique - Le droit civil à l'ère du numérique, actes du colloque du Master 2 Droit privé général et du Laboratoire de droit civil - Paris II - 21 avril 2017, La Semaine Juridique, Lexisnexis - Décembre 2017, page 36.

[1228] Art. 8 paragraphe 1 de la Charte des Droit Fondamentaux de l'Union Européenne.

[1229] CA Paris 15 mai 1970, D. 1970. Jur. 466, concl. Cabannes : Il a été précisé que l'identité est composée de tout ce qui permet d'individualiser une personne : le nom, le prénom, les coordonnées.

[1230] Lassalle M., étude, Droit à l'autodétermination informationnelle - La réparation des atteintes au droit à l'autodétermination informationnelle, Communication Commerce électronique n° 2, Février 2021, étude 4.

[1231] Deroudille A. et Fatah F., L'extraterritorialité du RGPD dans le contexte du « Cloud Act », Rev. UE 2019. n°442.

caractère personnel[1232]. L'inapplication du RGPD au contrat de cloud computing n'a aucune incidence sur la recevabilité d'une action judiciaire fondée sur l'atteinte au droit à la vie privée. La personne physique pourra engager une action en responsabilité contre le prestataire de services de cloud computing, agissant ou non en qualité de « responsable du traitement » ou de « sous-traitant ». Cette action concerne tout autant le prestataire de services cloud qui aura intégré dans son contrat de cloud computing une clause relative à une autorisation de traitement et de collecte des données personnelles que les contrats de cloud computing dépourvus d'une telle clause. Dans la situation où le RGPD s'avèrerait inadapté à la protection des données à caractère personnel dans le contrat cloud, la victime conserve la possibilité d'engager la responsabilité du prestataire de services cloud sur le fondement du droit à la vie privée.

***517. Une application jurisprudentielle étendue de la protection des données par le droit à la vie privée.*** Concernant l'appréciation de l'atteinte à la vie privée, la CJUE a considéré dans son arrêt en date du 11 décembre 2014 que « le traitement de données à caractère personnel susceptible de porter atteinte aux libertés fondamentales et, en particulier, au droit à la vie privée, doivent nécessairement être interprété à la lumière des droits fondamentaux qui sont inscrits dans la Charte des droits fondamentaux »[1233]. Le droit à la vie privée s'applique, ainsi, aux données personnelles qui se rattachent à la « vie privée » de la personne physique. Le droit à la protection des données à caractère personnel est étroitement lié au droit à la vie privée tel que considéré par la grande chambre de la CJUE dans sa décision en date du 9 novembre 2010[1234]. En l'espèce, la Cour avait considéré que « la publication sur un site Internet des données nominatives relatives aux bénéficiaires des fonds et aux montants perçus par ceux-ci constitue, en raison du libre accès par les tiers au site, une atteinte au droit des bénéficiaires concernés au respect de leur vie privée, en général, et à la protection de leurs données à caractère personnel, en particulier ». Elle ajoute que « pour être justifiée, une telle atteinte doit être prévue par la loi, respecter le contenu essentiel desdits droits et, en application du principe de proportionnalité, être nécessaire et répondre effectivement à des objectifs d'intérêt général reconnus par l'Union, les dérogations et limitations à ces droits devant s'opérer dans les limites du strict nécessaire». Cette jurisprudence européenne conforte le renforcement de la protection des données personnelles par la possibilité offerte à la personne physique d'utiliser le fondement juridique du droit à la vie privée.

---

[1232] Ibid.

[1233] CJUE, 4e ch. 11 décembre 2014, affaire n° C-212/13, František Ryneš c/ Úřad pro ochranu osobních údajů,: demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par le Nejvyšší správní soud (République tchèque).

[1234] CJUE 9 novembre 2010, Affaire Volker und Markus Schecke et Eifert : https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_fr.pdf.

***518.*** Il en résulte de cette analyse que le champ de la protection des données à caractère personnel est, ici, élargi par l'admission d'une action en responsabilité fondée sur l'atteinte au droit à la vie privée.

***519.*** Après avoir étudié la diversité des actions en responsabilité envisageables au profit, du client, personne physique, il convient d'étudier les réparations pouvant être accordées au profit de ce dernier.

## B) Le renforcement de la protection des données personnelles par une réparation étendue

***520.*** Le renforcement de la protection des données personnelles est envisagé à travers l'étude de la réparation accordée au client, personne physique, pour les préjudices résultant d'une atteinte au droit à la protection des données personnelles.

***521.*** **Plan.** Dans cette partie, il est envisagé d'étudier la réparation dans le cadre de l'application de la loi (2) et du contrat (2).

### 1) Une réparation étendue par la loi

***522.*** Le renforcement de la protection des données est opéré par un élargissement du champ de la réparation. L'élargissement du champ de la réparation est appréhendé dans le cadre d'une action fondée sur l'atteinte au droit à l'autodétermination informationnelle et au droit à la vie privée.

***523.*** **Plan.** Dans cette partie, il est envisagé d'étudier, pour chacune de ces actions, la réparation des préjudices en cas d'atteinte au droit à l'autodétermination informationnelle (a) et au droit à la vie privée (b).

a) La réparation des préjudices en cas d'atteinte au droit à l'autodétermination informationnelle

***524. La réparation du préjudice matériel et moral.*** Le principe du droit à réparation en cas d'atteinte au « droit à l'autodétermination informationnelle », dont les contours et la reconnaissance semblent encore incertains[1235], est affirmé à l'article 82 du RGPD, lequel dispose que « toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement, a le droit d'obtenir du responsable du traitement ou du sous-traitant la réparation du préjudice subi ». Le règlement consacre un droit à réparation au profit des personnes physiques dès lors qu'elles ont subi un préjudice issu d'une violation à leur droit à la protection des données à caractère personnel[1236]. En matière de cloud computing, dès lors que le prestataire de services cloud, qualifié de « responsable du traitement » a manqué aux obligations légales de protection des données à caractère personnel (RGPD) alors le client a droit à une réparation de son préjudice.

***525.*** Concernant les contours de ce droit à réparation, l'article 82 du RGPD vise aussi bien le dommage matériel que moral, mais la notion de préjudice moral n'a pas fait l'objet d'une définition harmonisée par le RGPD[1237]. La doctrine pose, alors, la question de savoir si une violation du RGPD entraine *de facto* une réparation au titre du préjudice moral[1238]. La jurisprudence est divisée sur ce point. Il est possible de considérer que « la seule violation du RGPD pourrait causer elle-même un préjudice moral indépendamment de tout autre dommage »[1239]. Cette position a été retenue par la jurisprudence britannique qui a appliqué le droit de l'Union européenne. En première instance, le tribunal britannique a considéré « qu'une action de groupe ne saurait prospérer sans la preuve que les personnes concernées ont subi des dommages matériels ou moraux »[1240], alors que la Cour d'appel britannique estime « au contraire que la perte de contrôle d'une personne sur ses données peut être considérée comme un

[1235] Lassalle M., étude, Droit à l'autodétermination informationnelle - La réparation des atteintes au droit à l'autodétermination informationnelle, Communication Commerce électronique n° 2, Février 2021, étude 4.

[1236] Danis-Fatôme A., étude, Protection des données - Quelles actions judiciaires en cas de violation du RGPD ?, Communication Commerce électronique n° 4, Avril 2018, dossier 18.

[1237] V. Art. 82.2 à 82.5 et cons. 85 du RGPD.

[1238] Lassalle M., étude, Droit à l'autodétermination informationnelle - La réparation des atteintes au droit à l'autodétermination informationnelle, Communication Commerce électronique n° 2, Février 2021, étude 4.

[1239] Ibid.

[1240] Lloyd v Google LLC [2018] EWHC 2599 (QB), dans Lassalle M., étude, Droit à l'autodétermination informationnelle - La réparation des atteintes au droit à l'autodétermination informationnelle, Communication Commerce électronique n° 2, Février 2021, étude.

préjudice en tant que tel »[1241]. Le raisonnement des juges dans cette affaire a été de considérer qui si l'exploitation des données des personnes a une valeur, dans ce cas la perte de contrôle d'une personne sur ses données devrait donc aussi avoir une valeur[1242]. Cette position a été saluée en doctrine comme favorisant l'effectivité du droit à l'autodétermination informationnelle des personnes physiques même en l'absence de dommage et ainsi contribuer au renforcement de la protection des données personnelles[1243]. La détermination du préjudice réparable suppose, donc, un équilibre entre plusieurs intérêts et nécessite de déterminer la finalité de la réparation[1244]. Il est encore difficile de limiter le champ d'application du droit à réparation des atteintes au droit à l'autodétermination informationnelle en raison que les recours ouverts visent à réparer « des atteintes à des intérêts abstraits dont il résulte essentiellement des préjudices intangibles »[1245].

***526. Les sanctions d'une atteinte au droit à l'autodétermination informationnelle***. Concernant le renforcement du droit à la réparation, l'atteinte au droit à la protection des données à caractère personnel est sanctionnée civilement, mais aussi pénalement dans certains cas graves. Les sanctions civiles se traduisent, tout d'abord, par l'imposition de sanctions pécuniaires[1246]. Afin de renforcer la protection des données personnelles, le RGPD a mis en place un mécanisme de contrôle[1247] et de saisine[1248] des autorités administratives[1249]. Dans le cadre de ses attributions,

---

[1241] Lloyd v Google [2019] EWCA Civ 1599, § 52 et 70, dans Lassalle M., étude, Droit à l'autodétermination informationnelle - La réparation des atteintes au droit à l'autodétermination informationnelle, Communication Commerce électronique n° 2, Février 2021, étude.

[1242] Ibid.

[1243] « Cette affaire britannique a le grand mérite de qualifier le problème : la perte du droit d'une personne de contrôler ce qui est fait de ses données. Elle est aussi remarquable car elle protège cet intérêt en l'absence de dommage. En effet, en 2015, une cour d'appel avait déjà reconnu l'existence d'un intérêt protégé nouveau (misuse of private information) distinct de la protection plus traditionnelle de la confidentialité (breach of confidence) mais il était alors question de réparer le préjudice moral (distress) qui découlait de l'atteinte à cet intérêt (*Google Inc v Vidal-Hall [2015] EWCA Civ 311*. Dans un contexte autre que celui de la protection des données, une juridiction avait toutefois reconnu le droit à réparation de l'atteinte au droit de contrôle sur des informations privées, en l'absence de dommage *(Gulati v MGN Limited [2015] EWHC 1482 (Ch))*. Cette fois, il n'est plus question de réparer un préjudice moral, qui devrait être prouvé, mais de considérer que la perte de contrôle sur les données cause elle-même un préjudice. Cette approche risque toutefois de soulever des problèmes de définition. Par exemple, le juge fonde une partie de son argumentation sur le considérant n° 85 du RGPD qui mentionne le préjudice causé par la perte de contrôle d'une personne sur ses données dans le seul contexte des violations de données à caractère personnel. De même, le droit anglais prévoit un critère de gravité (seriousness) dans les recours visant à engager la responsabilité de responsables du traitement (*Lloyd v Google [2019] EWCA Civ 1599, § 55.)*. Cela illustre le fait que la reconnaissance du droit à réparation nécessite que celui-ci soit délimité » : Lassalle M., étude, Droit à l'autodétermination informationnelle - La réparation des atteintes au droit à l'autodétermination informationnelle, Communication Commerce électronique n° 2, Février 2021, étude 4.

[1244] Mekki M., La place du préjudice en droit de la responsabilité civile : Hokkaïdo Journal of New Global Law and Policy, vol. 5, 2010, p. 151-200.

[1245] Lassalle M., étude, Droit à l'autodétermination informationnelle - La réparation des atteintes au droit à l'autodétermination informationnelle, Communication Commerce électronique n° 2, Février 2021, étude 4.

[1246] V. art 58, 2) du RGPD.

[1247] V. art. 51 et 58, 1) du RGPD.

la formation restreinte de la CNIL peut prononcer, à l'issue de contrôles ou de plaintes, des sanctions pécuniaires en cas de violations des obligations du RGPD. Les conditions pour l'imposition de ces amendes administratives sont prévues l'article 83 du RGPD. Il est précisé que l'établissement de la sanction pécuniaire prend en compte plusieurs critères tels que la gravité et la durée de la violation, les mesures prises pour atténuer le dommage subi par les personnes concernées, le degré de coopération (..). Le montant des amendes varie en fonction du type de violation, il est prévu qu'en présence d'une violation des principes de traitement des données ou le non-respect des conditions de licéité du traitement, l'amende s'élève à 20 millions d'euros ou 4 % du chiffre d'affaires dans le cas d'une entreprise[1250]. Ces sanctions pécuniaires doivent être proportionnées au regard du type de violation[1251]. Au regard, du montant de l'amende (20 millions d'euros ou 4 % du chiffre d'affaires), ces sanctions pécuniaires contribuent au renforcement de la protection des données dans les contrats de cloud computing par l'effet dissuasif qu'elles peuvent générer auprès des prestataires de services cloud (et ce en leur qualité de responsable du traitement). Outre les amendes administratives (article 82 RGPD), le prestataire de services cloud peut être condamné, dans le cadre d'un recours juridictionnel exercé à titre individuel[1252] ou collectif (action de groupe)[1253], à verser au client, personne physique, des dommages et intérêts en réparation des préjudices subis. Dans certaines situations, les sanctions civiles peuvent être complétées par d'autres mesures matérielles telles que le séquestre, la confiscation.

***527.*** Des sanctions pénales sont également prévues en application de l'article 84 du RGPD. Cet article confère aux États membres le pouvoir de mettre en place des sanctions supplémentaires en cas de violation du RGPD, lesquelles ne font pas l'objet d'amendes administratives. À ce titre, la France a inséré au sein de son Code pénal de nombreuses sanctions liées au traitement de données personnelles. À titre illustratif, l'article 226-21 du Code pénal prévoit, en cas de détournement de la finalité lors du traitement de données personnelles, une peine de 5 ans d'emprisonnement et 300 000 euros d'amende. Les sanctions pénales emportent une sanction financière et/ou une peine d'emprisonnement, mais la peine d'emprisonnement est réservée dans les cas les plus graves[1254]. Pour renforcer le droit à réparation, les juges ont appliqué dans

---

[1248] Il s'agit du droit des personnes physiques d'introduire une réclamation auprès d'une autorité de contrôle prévu à l'article 77 du RGPD.

[1249] En France, il s'agit de la CNIL.

[1250] V. art. 85 RGPD.

[1251] Illustration de sanctions pécuniaires prononcées par la CNIL : Elle a infligé le 6 juin 2019 la sanction de 400 000 euros à l'encontre de la société SERGIC (…) pour avoir insuffisamment protégé les données des utilisateurs de son site web et mis en œuvre des modalités de conservation des données inappropriées.

[1252] V. *supra* n° 490 et suivants.

[1253] V. *supra* n° 504 et suivants.

[1254] Exemple, la divulgation du secret par les professionnels.

certaines affaires les dispositions du Code pénal relatives aux délits de vol sur le fondement de l'article 311-1 du code pénal[1255], d'escroquerie sur le fondement de l'article 313-1 du code pénal, d'abus de confiance sur le fondement de l'article 314-1 du code pénal[1256], de destruction, dégradation ou détérioration de biens appartenant à autrui sur le fondement des articles 322-1 et 322-6 du code pénal, de faux et d'usage de faux sur le fondement de l'article 441-1 du code pénal afin de sanctionner les atteintes portées au droit à la protection des données.

***528.*** Après avoir envisagé la réparation des préjudices résultant d'une atteinte au droit à l'autodétermination informationnelle, il est envisagé à présent d'étudier la réparation des préjudices sur le fondement de l'atteinte au droit à la vie privée.

b) La réparation des préjudices en cas d'atteinte au droit à la vie privée

***529. La réparation de l'atteinte au droit à la vie privée en l'absence de préjudice***. La question se pose, ici, de savoir si une personne physique est en mesure d'obtenir une réparation en cas d'atteinte à son droit à la vie privée en l'absence même de tout préjudice. À cette question, la réponse est que le droit à la vie privée est un droit de la personnalité et qu'en application de l'article 9 du Code civil, il ouvre droit à réparation sans preuve d'un préjudice. La doctrine considère sur ce point que « la difficulté n'est donc pas de déterminer un préjudice, il peut ne pas y en avoir, mais de définir ce qui constitue une atteinte au droit à la vie privée »[1257]. Dès lors que la donnée à caractère personnel est considérée comme relevant de la sphère de la « vie privée », la personne physique peut demander une réparation en l'absence même d'un préjudice, ce qui permet de renforcer considérablement la protection des données à caractère personnel. En revanche, pour les autres données à caractère personnel considérées comme ne relevant pas du domaine de la vie privée de la personne, alors la recevabilité de l'action en réparation fondée sur l'atteinte au droit à la protection des données à caractère est conditionnée à la preuve d'un préjudice soit matériel soit moral en application de l'article 82 du RGPD[1258]. Cette exclusion est accueillie favorablement par certains auteurs qui considèrent : « que toutes les données

[1255] V. arrêt de la Chambre criminelle portant sur le vol et le recel de fichiers clients d'un ancien employeur : Cass. crim., 20 oct. 2010, pourvoi nº 09-88.387.

[1256] Illustration concernant le vol de données numériques, TGI Clermont-Ferrand, ch. Corr., 26 sept. 2011 : le tribunal qualifie de vol et d'abus de confiance le fait pour une salariée de transférer le jour de son départ de l'entreprise, des données informatiques confidentielles afin de les utiliser à des fins personnelles.

[1257] Laulom S., L'indépendance affirmée de l'article 9 du Code civil du droit commun de la responsabilité : D. 1997, p. 403- Dans Lassalle M., étude, Droit à l'autodétermination informationnelle - La réparation des atteintes au droit à l'autodétermination informationnelle, Communication Commerce électronique n° 2, Février 2021, étude 4.

[1258] Article 82 du RGPD dispose que « toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement, a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi ».

personnelles ne sont pas assez privées pour être protégées par le droit à la vie privée »[1259]. Il est mis en lumière qu'en fonction de la nature de la donnée, celle-ci puisse être considérée comme portant ou non atteinte au droit à la vie privée et donc au droit de la personnalité permettant d'obtenir une réparation sans apporter la preuve d'un préjudice. Il en découle de cette analyse que le client, personne physique, peut prétendre à obtenir réparation de l'atteinte, par le prestataire de services cloud, à son droit à la vie privée sans la nécessité de démontrer l'existence d'un préjudice. À titre illustratif concernant l'atteinte au droit à la vie privée, la CNIL a constaté, dans le cadre de son contrôle, que la société Google a procédé à une collecte de données supérieure à ce qui était prévu dans les conditions générales d'utilisation. Elle a, donc, sanctionné une telle collecte excessive pour défaut de transparence dans le traitement et absence de consentement valide en tant qu'atteinte au droit à la vie privée des personnes concernées. Elle a estimé que ces manquements constituent « des atteintes substantielles à la protection de leur vie privée et se situent à contre-courant des aspirations légitimes des personnes souhaitant conserver la maîtrise de leurs données »[1260].

***530. Les sanctions d'une atteinte au droit à la vie privée***. À l'instar des autres droits fondamentaux, ce droit bénéficie d'une protection juridique se traduisant par la possibilité d'intenter une action judiciaire. Le responsable encourt, ici, des sanctions de nature civile et pénale. Concernant les sanctions civiles, la personne qui a porté atteinte au droit à la vie privée encourt le versement de dommages et intérêts au profit de la personne concernée par cette atteinte. C'est le juge qui fixe le montant en fonction de la gravité de la situation. D'autres mesures civiles peuvent être prononcées pour prévenir ou faire cesser l'atteinte au droit à la vie privée, par exemple, la suppression de la communication diffusée publiquement portant atteinte au droit à la vie privée, le séquestre (..). Concernant les sanctions pénales, il est prévu à l'article 226-1 du Code pénal que l'auteur est sanctionné par un an d'emprisonnement et une amende de 45 000 euros lorsque l'intimité de la vie privée a été atteinte : « 1° en captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ; 2° en fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé ». Également, l'article 226-3 du même code énonce que « la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques permettant la réalisation du délit d'atteinte à

[1259] Deschanel C., L'instauration d'un droit de propriété des données personnelles ? : vrai danger ou fausse utilité ? : RLDI n° 156, 2019, n° 5344. – Destreguil M., Plaidoyer en faveur d'une approche propriétariste des données personnelles : RJFP n° 3, 2019. Dans Lassalle M., étude, Droit à l'autodétermination informationnelle - La réparation des atteintes au droit à l'autodétermination informationnelle, Communication Commerce électronique n° 2, Février 2021, étude 4.

[1260] CNIL, délib. de la formation restreinte n° SAN – 2019-001, 21 janv. 2019 prononçant une sanction pécuniaire à l'encontre de la société Google LLC, in Lassalle M., étude, Droit à l'autodétermination informationnelle - La réparation des atteintes au droit à l'autodétermination informationnelle, Communication Commerce électronique n° 2, Février 2021, étude 4.

l'intimité est passible de 300 000 euros d'amende et de 5 ans d'emprisonnement ». Toutes ces sanctions peuvent s'appliquer à un prestataire de services cloud dans le cadre de l'exécution d'un contrat cloud conclu avec une personne physique dès lors que les conditions de l'atteinte au droit à la vie privée sont remplies.

***531.*** En définitive, qu'il s'agisse des sanctions fondées sur une atteinte au droit à la protection des données à caractère personnel ou au droit à la vie privée, des sanctions civiles et pénales sont prévues, lesquelles permettent de renforcer la protection des données à caractère personnel par l'effet dissuasif qu'elles génèrent, à destination des prestataires de services cloud dans le cadre de l'exécution d'un contrat de cloud computing. La protection des données à caractère personnel se trouve, ainsi, renforcée en raison de l'admission d'une réparation du préjudice matériel et moral (dans le cadre d'une atteinte au droit à l'autodétermination informationnelle) ainsi que la réparation en l'absence même d'un préjudice (dans le cadre d'une atteinte au droit à la vie privée) et l'imposition de sanctions.

***532.*** Après avoir étudié, le renforcement du droit à réparation par l'extension du champ de la réparation, il est envisagé désormais d'étudier le renforcement du droit à réparation par le contrat cloud.

**2) Une réparation fondée sur le contrat cloud**

***533.*** Dans le cadre de l'exécution du contrat cloud, la personne physique peut engager au lieu et place de la responsabilité délictuelle du prestataire, la responsabilité du prestataire de services cloud en cas de manquements à ses obligations contractuelles en matière de protection des données personnelles. Le client, personne physique, devra se référer au contrat de cloud computing qui fait office de « loi des parties »[1261] afin d'identifier le régime de la responsabilité contractuelle applicable au prestataire de services. Le client peut intenter une action en responsabilité contractuelle contre le prestataire de service de cloud computing dès lors que ce dernier a manqué à ses obligations contractuelles et après avoir adressé une mise en demeure de remédier à ces manquements[1262]. Dans le cadre de cette action, la question se pose du droit à réparation de la personne physique pour le préjudice subi résultant d'un manquement par le prestataire de ses obligations contractuelles et en particulier d'un manquement au droit à la protection des données personnelles. Il s'agit d'identifier la nature et la gravité du manquement

[1261] V. art. 1103 du code civil : « Les contrats légalement formés tiennent lieu de loi à ceux qui les ont faits ».

[1262] V. art. 1231 C. civ. concernant la mise en demeure.

à l'obligation contractuelle. Dans cette configuration, il s'agit d'identifier dans le contrat de cloud computing quelles sont les obligations incombant au prestataire de services cloud et quelles sont les sanctions prévues en cas de manquement. En matière contractuelle, seuls les dommages prévisibles peuvent être indemnisés[1263]; par conséquent, le client, personne physique, devra être vigilant quant au contenu du contrat et en particulier aux clauses relatives à la responsabilité.

***534.*** Il est question de vérifier, dans le contrat de cloud computing, l'existence ou non d'une clause limitative ou élusive de responsabilité[1264]. En cas de présence d'une clause limitative de responsabilité, il faut analyser si celle-ci a pour effet de restreindre très fortement la possibilité de mettre en œuvre la responsabilité du prestataire de services cloud. En cas de réponse positive, il sera possible de demander au juge de la déclarer comme étant une clause abusive afin de la priver d'effet. À titre d'exemple, les sociétés Google et Apple ont inséré, dans leurs contrats cloud, des clauses limitatives et élusives de responsabilités. En fonction de la nature du contrat (contrat d'adhésion) et la manière dont les clauses sont rédigées, il sera plus ou moins possible de demander aux juges de les priver d'effets juridiques en prononçant la sanction du « réputé non écrit »[1265].

***535.*** Le client, personne physique, peut contester une clause limitative ou élusive de responsabilité, dès lors que celle-ci constitue une clause abusive établissant un déséquilibre significatif entre les droits et les obligations des parties. À titre illustratif dans le contrat d'Apple, il est spécifié qu'Apple ne peut être tenue responsable envers l'utilisateur de « tout dommage direct, indirect, accidentel, particulier, immatériel ou exemplaire, y compris sans s'y limiter, les dommages pour perte de profits, de clientèle, d'utilisation, de données, de coûts d'acquisition de biens ou services de remplacement, ou toute autre perte intangible (…)»[1266]. Par cette disposition contractuelle, Apple ne pourrait pas être tenue responsable en cas de pertes de données. L'utilisateur du service i-cloud ne peut donc se retourner contre Apple pour obtenir une indemnisation à la suite de la perte de ces données puisque c'est à lui qu'incombe l'obligation de sécuriser son compte i-cloud.

***536.*** Si en matière de responsabilité contractuelle, l'indemnisation du dommage « prévisible » est la règle ; la personne physique peut toujours demander aux juges de statuer sur cette clause limitant le montant de l'indemnisation du dommage dès lors qu'il s'agit d'une restriction excessive[1267]. À titre illustratif, dans le contrat cloud de Google, il est mentionné expressément

---

[1263] V. art. 1231-3 C. civ. relatif à l'indemnisation du préjudice prévisible.

[1264] V. *supra* n° 149 et suivants sur l'étude des clauses limitatives et élusives de responsabilités dans les contrats cloud.

[1265] V. *supra* n° 154 et suivants.

[1266] Contrat i.cloud d'Apple : https://www.apple.com/legal/internet-services/icloud/fr/terms.html.

[1267] V. art. 1231-3 C. civ.

dans les conditions d'utilisation, que Google décline toute responsabilité pour les pertes de données, que dès lors que la responsabilité de Google serait retenue l'indemnisation est limitée au montant que l'utilisateur à payer pour utiliser les services, que Google, ses fournisseurs et distributeurs, ne seront tenus responsables pour toute perte ou tout dommage qui n'aurait pas été raisonnablement prévisible[1268]. Si ces dispositions constituent des restrictions pour la mise en œuvre du droit à réparation des clients, personnes physiques, Google tempère la portée de ces dispositions en précisant que « Si vous utilisez les Services pour un usage personnel, aucune disposition des présentes Conditions d'Utilisation ou des conditions d'utilisation supplémentaires ne limite les droits légaux du consommateur auxquels aucun contrat ne peut déroger »[1269]. Cette disposition est directement applicable en faveur des clients, personnes physiques, qui utilisent les services cloud pour un usage personnel.

***537.*** Dans le cadre de l'affaire opposant l'association de consommateurs UFC Que Choisir et la société Twitter Inc[1270], les juges ont déclaré plusieurs clauses des conventions d'utilisation comme étant abusives. Ces clauses déclarées abusives avaient « pour objet de limiter la responsabilité du réseau social (sur les contenus des publications, en cas de dysfonctionnement du service, en cas de piratage du compte), de lui octroyer un pouvoir « trop discrétionnaire » (contenus à supprimer, résiliation du compte, modification unilatérale des conditions) et d'entraver l'exercice des droits du consommateur (loi applicable et attribution de juridiction en Californie, manque de clarté des stipulations) »[1271]. En particulier, la clause qui prévoit « une résiliation des services à l'initiative de Twitter, de manière discrétionnaire à tout moment sans justification ni préavis en conséquence, dès qu'une enquête est menée, sans en attendre les éventuelles conclusions et sans permettre à l'utilisateur de s'y opposer ou de fournir des explications en défense », a été déclarée comme abusive en raison qu'elle « crée au profit du professionnel et au détriment du consommateur ou du non-professionnel un déséquilibre significatif au sens de l'article L. 132-1 devenu l'article L. 221-1 du code de la consommation »[1272].

***538.*** Dans le cade de l'affaire Facebook[1273], les juges ont été amené à statuer sur la clause attributive de compétence juridictionnelle contenue dans les conditions générales de la déclaration des droits et responsabilités de Facebook. En l'espèce, les juges ont constaté que

[1268] V. contrat cloud de Google : https://policies.google.com/terms.

[1269] Ibid.

[1270] TGI Paris, 7 août 2018, affaire Twitter n° 14/07300.

[1271] Le Tourneau Ph., Contrats du numérique, informatiques et électroniques, Dalloz, 12e édition 2022/2023, chap. 011 Prolégomènes, Section 2 - Limites des révolutions induites par l'informatique et par l'internet (011.81 - 011.89) (1).

[1272] TGI Paris, 7 août 2018, *op. cit.*

[1273] CA Paris 12 février 2016, affaire n°15/08624.

cette clause « oblige le souscripteur, en cas de conflit avec la société, à saisir une juridiction particulièrement lointaine et à engager des frais sans aucune proportion avec l'enjeu économique du contrat souscrit pour des besoins personnels ou familiaux ; que les difficultés pratiques et le coût d'accès aux juridictions californiennes sont de nature à dissuader le consommateur d'exercer toute action devant les juridictions concernant l'application du contrat et à le priver de tout recours à l'encontre de la société Facebook Inc ; qu'à l'inverse, cette dernière a une agence en France et dispose de ressources financières et humaines qui lui permettent d'assurer sans difficulté sa représentation et sa défense devant les juridictions françaises »[1274]. En se fondant sur cette appréciation factuelle des effets de cette clause et sur l'article R. 132-2 du code de la consommation qui présume abusives les clauses ayant pour objet de « supprimer ou entraver l'exercice d'actions en justice ou des voies de recours par le consommateur »., les juges ont considéré que « la clause attributive de compétence juridictionnelle au profit des juridictions californiennes contenue dans le contrat a pour effet de créer, au détriment du non-professionnel ou du consommateur, un déséquilibre significatif entre les droits et obligations des parties au contrat ; qu'elle a également pour effet de créer une entrave sérieuse pour un utilisateur français à l'exercice de son action en justice »[1275].

***539.*** Également, si une clause pénale[1276] est prévue au contrat de cloud computing, le client, personne physique, a la faculté de demander aux juges de l'appliquer avec la possibilité réservée aux juges de réviser le montant si celle-ci est excessive ou dérisoire[1277]. En principe (étant dans un contrat d'adhésion), s'il existe une clause pénale, celle-ci sera rédigée en faveur du prestataire de services cloud et non du client, personne physique. Dans cette hypothèse, le client pourra demander au juge de réviser le montant de cette clause pénale si l'indemnisation est dérisoire. En outre, le client dispose toujours la faculté de demander aux juges des dommages-intérêts compensatoires[1278] pour le préjudice subi dont le montant de cette allocation dépendra de la nature et de la gravité du manquement à cette obligation contractuelle. Les clients, personnes physiques, peuvent, également, intenter une action de groupe[1279] contre le prestataire de services cloud,[1280] et ce afin d'obtenir la réparation des préjudices patrimoniaux résultant des dommages matériels.

---

[1274] CA Paris 12 février 2016, *op. cit.*

[1275] CA Paris 12 février 2016, *op. cit.*

[1276] V. art. 1226 C. civ. dans sa rédaction de 1804.

[1277] V. art. 1231-5 C. civ. V. Cass. com 20 déc. 2017 n°16-18.280 non publié au bulletin : dans cet arrêt la Cour rappelle que les juges du fond disposent d'un pouvoir souverain d'appréciation du caractère manifestement excessif (ou dérisoire) de la clause pénale.

[1278] V. art.1231-6 C. civ.

[1279] V. les art. L. 623-1 à L. 623-32 C. consom.

[1280] V. art. L. 623-1 C. consom.

***540.*** En définitive, il apparaît que dans le cadre d'un contexte européen, la protection des données est renforcée par la possibilité au client (personne physique) d'engager des actions contre le prestataire de services cloud et/ou son sous-traitant en responsabilité fondées sur des manquements aux prescriptions légales et contractuels.

***541.*** Après avoir étudié les responsabilités élargies dans un contexte européen, lesquelles permettent de renforcer la protection des données à caractère, il est envisagé d'étudier l'application de ces règles européennes protectrices dans un contexte international. En particulier, l'étude du droit applicable et de la compétence juridictionnelle.

## Section 2. L'élargissement des responsabilités dans un contexte international

***542. L'ubiquité des données et les conflits de lois.*** Par cette localisation des données hors des frontières de l'Union européenne, ce sont les droits fondamentaux des utilisateurs, personnes physiques, qui risquent de s'en trouver affaiblis et notamment le droit à la protection des données à caractère personnel et le droit d'accès à la justice. La difficulté juridique, dans le cadre de la technologie du cloud, est de pouvoir déterminer quels sont les droits applicables et la juridiction compétente. Concernant la caractéristique des données stockées dans le cloud, le Professeur Delmas-Marty la nomme « l'ubiquité »[1281] et cette notion d'ubiquité permet d'illustrer cet espace virtuel dans lequel sont stockées et traitées des données et sans que les frontières soient un frein à leur transfert. En effet, « pour des raisons technologiques et économiques, les activités humaines dépassent de plus en plus fréquemment les frontières des États. Cet état de fait remet en cause les coutumes internationales relatives à l'étendue des compétences édictives et adjudicatives des États »[1282]. Cette virtualisation bouleverse nos raisonnements juridiques classiques en matière de détermination du droit applicable et de compétence juridictionnelle. Cette difficulté à saisir quel est le droit applicable en matière de transfert des données est propre au domaine des nouvelles technologies de l'information et de la communication et en particulier de la technologie du Cloud. Dans ce contexte, la question de la portée du principe de l'applicabilité extraterritoriale du droit européen de la protection des données est régulièrement soulevée[1283]. Afin d'étendre la réglementation européenne, hors des

[1281] La notion « d'ubiquité », en raison que les données sont stockées dans un espace virtuel libre et qu'il est très difficile en pratique de localiser ces données. V. également, Delmas-Marty M., Le relatif et l'universel. Les forces imaginantes du droit, Ed. du Seuil, 2004, p. 337.

[1282] Rigaux F. et Delpérée F., Le concept du peuple, 1re éd., Bruxelles, Story-Scienta, 1988, p. 216.

[1283] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, Revue internationale de droit économique 2019/4 (t. XXXIII), p. 503.

frontières de l'Union européenne et permettre ainsi d'élargir le champ de la protection des données à caractère personnel (et notamment les règles permettant d'engager la responsabilité), il est question d'étudier les règles en matière d'extraterritorialité. L'objectif étant d'étendre le champ d'application de la réglementation européenne, hors des frontières de l'Union européenne, et de permettre aux personnes physiques d'agir contre des responsables établis hors des frontières de l'Union européenne.

***543.*** ***Plan***. L'étude du renforcement de la protection des données personnelles par un élargissement des responsabilités au niveau international s'appuiera, d'une part, sur l'application extraterritoriale du RGPD (A) et de la compétence juridictionnelle (B).

## A) Le renforcement de la protection des données par l'application extraterritoriale du RGPD

***544.*** Avant l'entrée en vigueur du RGPD et dans le cadre d'un transfert de données personnelles en dehors des frontières de l'espace économique européen (l'EEE), il s'était posé la question de l'application territoriale de la législation européenne. La directive européenne de 1995[1284] énonçait les principes relatifs au droit applicable, mais ce texte n'était pas d'application directe dans les États ; il était nécessaire de passer par une transposition de ces principes en droit interne[1285]. À ce titre, la règle consistait en l'application du droit national, lequel devait être établi en vertu des principes énoncés par la Directive. Des incertitudes ont été soulevées devant les juges concernant l'application des critères pour la détermination du droit applicable. Sur ce point, la CJUE est intervenue et a donné sa position dans un arrêt en date du 13 mai 2014[1286] dans lequel elle a jugé « qu'un traitement de données à caractère personnel est effectué dans le cadre des activités d'un établissement du responsable de ce traitement sur le territoire d'un État membre, au sens de la directive 95/46/CE, lorsque l'exploitant d'un moteur de recherche, bien qu'ayant son siège dans un État tiers, crée dans un État membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publicitaires proposés par ce moteur et dont l'activité vise les habitants de cet État membre ». En d'autres termes, dès lors que les activités de l'exploitant du moteur de recherche et celles de son établissement se trouvent dans un État membre, la législation européenne a vocation à s'appliquer. Les juges décident, alors,

[1284] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[1285] V. art.4, Directive 95/46/CE.

[1286] CJUE 13 mai 2014 (grande chambre), Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, aff. C-131/12.

d'appliquer la réglementation européenne relative à la protection des données à une situation qui de prime abord semblerait échapper à la réglementation européenne dès lors que les activités du « professionnel » se trouvent dans un État membre. Dans cette situation, le droit à la réparation des victimes d'une atteinte au droit à la protection des données s'en est trouvé renforcer par la jurisprudence[1287] avant de l'être, aujourd'hui, par le RGPD.

***545.*** Pour pallier ces difficultés d'un conflit de lois, le RGPD a apporté des clarifications en matière de droit applicable afin de rendre effectif le droit à réparation des personnes physiques en cas d'atteinte au droit à la protection des données personnelles. À la différence de la Directive de 1995[1288], l'article 3 du RGPD définit le champ d'application territoriale d'un texte directement applicable dans l'ordre juridique interne des États membres de l'Union européenne. Il est rappelé que « le RGPD engage plusieurs États et s'applique sur la somme des territoires des États partis ou sur l'espace juridique des États contractants »[1289] . Cette disposition prévoit un champ d'application territorial étendu du règlement, et ce afin d'assurer un niveau élevé de protection des données personnelles et de sécurité juridique. Concernant le champ d'application, il est posé deux critères alternatifs, à savoir, le critère d'« établissement», et le critère de «ciblage»[1290].

***546.*** Le critère d'établissement permet d'appliquer le RGPD en présence d'un traitement de données « effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union » alors même que le traitement a lieu ou non dans l'Union »[1291]. La notion d'établissement, ici, suppose « l'exercice effectif et réel d'une activité au moyen d'un dispositif stable »[1292] et ce « quelle que soit la forme juridique de ce dispositif (succursale ou filiale, selon le considérant 22 du RGPD) »[1293]. En l'espèce, le RGPD s'applique dès lors que l'établissement du responsable du traitement ou un sous-traitant se situe sur le territoire de l'Union. Ce critère de rattachement par la localisation de l'établissement s'inscrit dans la continuité de la jurisprudence européenne. La CJUE, dans son arrêt du 1er

---

[1287] Ibid.

[1288] V. art.4, Directive 95/46/CE.

[1289] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p. 512, *op. cit.*. V. également, CEDH, 12 décembre 2001, Bancovic et autres c. la Belgique, la République tchèque, le Danemark, la France, l'Allemagne, la Grèce, la Hongrie, l'Islande, l'Italie, le Luxembourg, les Pays-Bas, la Norvège, la Pologne, le Portugal, l'Espagne, la Turquie et le Royaume-Uni, n° 55207/99, considérant 80.

[1290] CEPD, Lignes directrices 3/2018 relatives au champ d'application territorial du RGPD (article 3), 12 novembre 2019. Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, Revue internationale de droit économique 2019/4 (t. XXXIII), p.502. V., également, Thierache C., « RGPS vs Cloud Act : le nouveau cadre légal américain est-il anti RGPD ? », Dalloz IP/IT, juin 2019, n° 6, p. 367.

[1291] V. art. 3 paragraphe 1 du RGPD qui détermine l'applicabilité du RGPD à raison de la localisation de l'établissement du responsable du traitement ou du sous-traitant.

[1292] CEPD, Lignes directrices 3/2018 relatives au champ d'application territorial du RGPD (article 3), *op. cit.*.

[1293] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p. 506, *op. cit.*.

octobre 2015[1294], « a retenu l'existence d'un établissement en présence d'un représentant, d'un compte bancaire et d'une boîte aux lettres »[1295]. Également, dans une autre affaire, la CJUE a jugé « que le droit espagnol transposant la directive 95/46/CE s'appliquait aux activités de Google, bien que l'établissement principal de Google se situait aux États-Unis »[1296]. Cette décision est prise à raison que l'une des filiales de la société Google était établie en Espagne et cela a permis de qualifier « d'établissement » (au sens de la Directive) la filiale espagnole de Google. La CJUE a, dans cette décision, une interprétation extensive de la notion « d'établissement » en considérant que celle-ci s'étend « à toute activité réelle et effective, même minime, exercée au moyen d'une installation stable ». En revanche, le lieu du traitement effectif des données est sans incidence sur l'application ou non du RGPD. Ce détachement concernant le lieu du traitement permet de prendre en compte les impératifs de protection des données personnelles en matière de cloud computing et d'étendre, ainsi, une application extraterritoriale du RGPD[1297] . Le RGPD constitue une évolution bénéfique au renforcement du droit à la protection des données personnelles par l'établissement de ce critère qui opère une extension de son champ d'application aux traitements réalisés par des sous-traitants[1298]. À titre illustratif, si un prestataire de service cloud, qualifié de responsable du traitement, est établi dans un pays hors de l'Union européenne, « ses activités de traitement pourront entrer dans le champ d'application territorial du RGPD, dès lors qu'il recourt à un sous-traitant établi dans l'UE pour collecter, analyser ou stocker des données personnelles »[1299].

***547.*** Concernant cette fois, le critère de ciblage, il permet d'appliquer le RGPD lorsqu'un responsable de traitement ou un sous-traitant non établi dans l'Union effectue un traitement de données à caractère personnel des personnes physiques situées sur le territoire lié à une offre de biens ou de services (y compris le contrat dit « gratuit »)[1300] ou au suivi de comportement qui a lieu au sein de l'Union[1301]. Il s'agit, ici, d'une application extraterritoriale du texte[1302] puisqu'il a vocation à s'appliquer aux responsables du traitement ou aux sous-traitants qui ne sont pas

[1294] CJUE, 1er octobre 2015, affaire n° C-230/14, Weltimmo.

[1295] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p. 507, *op. cit.*.

[1296] CJUE 13 mai 2014 (grande chambre), Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, aff. C-131/12.

[1297] Métille S., « L'utilisation de l'informatique en nuage par l'administration publique », AJP/PJA, juin 2019

[1298] V. Poullet Y., La vie privée à l'heure de la société du numérique, 1re éd, Bruxelles, Larcier, 2019, p. 5.

[1299] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p. 508, *op. cit.*.

[1300] Pour apprécier ce critère, la CJUE utilise un faisceau d'indices tels que l'usage de « la monnaie européenne, l'emploi d'une des langues nationales d'un pays membre, la livraison sur le territoire de l'Union » : v. CJUE, 7 décembre 2010, Peter Pammer c. Reederei Karl Schülter GmbH & Co. KG et Hotel Alpenhof GmbH c. Oliver Heller, aff. C-585/08 et C-144/09, pt. 70 et s.

[1301] V. art.3 paragraphe 2 du RGPD qui détermine l'applicabilité du RGPD à raison de la localisation des personnes concernées par le traitement sur le territoire de l'Union.

[1302] V. *supra* n° 180 et suivants.

établis dans l'UE, lorsque les traitements visent des personnes dans l'Union et sont liés à des offres de biens ou de services (même gratuits) dans l'Union, ou au profilage du comportement de ces personnes sur le territoire de l'Union. Tel qu'affirmé par Madame Thelisson, l'application de « ce second critère contraint potentiellement de nombreux acteurs établis hors de l'Union »[1303]. À titre illustratif, la CJUE a confirmé dans le cadre d'une saisine par l'autorité de contrôle autrichienne contre une entreprise établie en Suisse[1304] « l'effectivité du contrôle *a posteriori*[1305], même en présence d'un élément d'extranéité »[1306] ; il en résulte de cette affaire qu'une entreprise suisse (État tiers à l'Union européenne) est soumise à l'application du RGPD dès lors que les conditions de l'article 3, al. 2 sont remplies. La portée extraterritoriale du RGPD atteste la volonté du législateur de renforcer le droit à la protection des données afin de protéger les personnes situées dans l'UE dont les données sont traitées, et ce indépendamment de la localisation effective du traitement. Il s'agit, donc, d'une protection élargie à toutes les personnes concernées qui se trouvent dans l'Union européenne.

***548.*** Dès lors que l'un de ces deux critères est rempli, les dispositions du RGPD s'appliquent au traitement de données personnelles effectué par le responsable du traitement ou le sous-traitant concerné[1307]. Ces critères permettent une extension du champ d'application de la réglementation européenne. En sus de ces deux critères, il est ajouté que le RGPD s'applique au traitement de données personnelles lorsque le droit d'un État membre s'applique en vertu du droit international public,[1308] lequel figurait déjà dans la Directive 95/46/CE[1309].

***549.*** Des auteurs ont catégorisé ces critères de l'article 3 du RGPD en « deux critères de localisation géographique définis par rapport au territoire de l'Union : le lieu d'établissement du responsable du traitement ou du sous-traitant, et la localisation des personnes concernées par le traitement »[1310]. Le RGPD est perçu par la doctrine comme étant une « innovation majeure » puisque « ce texte va s'appliquer indépendamment du lieu de traitement effectif des données. Il

---

[1303] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p. 502, *op. cit.*. V. également, Pailler L., « L'applicabilité spatiale du Règlement général sur la protection des données (RGPD) : Commentaire de l'article 3 », JDI, 2018, p. 829.

[1304] CJUE, 3 septembre 2008, Kadi, affaires n° C-402/05 P et C-415/05 P.

[1305] Il s'agit de la coopération internationale à travers le mécanisme du guichet unique de l'art.56 du RGPD.

[1306] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p. 519, *op. cit.*.

[1307] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p. 502, *op. cit.*.

[1308] V. art. 3 paragraphe 3 du RGPD qui étend l'application du RGPD aux établissements situés hors de l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public. V. Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, Revue internationale de droit économique 2019/4 (t. XXXIII), p. 503. V. également, Pailler L., « L'applicabilité spatiale du Règlement général sur la protection des données (RGPD) : Commentaire de l'article 3 », JDI, 2018, p. 829.

[1309] V. article 4.1, a et b, Directive 95/46/CE qui énonçait l'application de la directive 95/46/CE au responsable du traitement « qui n'est pas établi dans l'Union, mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public ».

[1310] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p. 519, *op. cit.*. Également, v. Pailler L., « L'applicabilité spatiale du Règlement général sur la protection des données (RGPD) : Commentaire de l'article 3 », JDI, 2018, p. 829.

s'agit, donc, d'une extension de l'applicabilité spatiale du texte. Le territoire sur lequel les activités de traitement des données sont effectuées n'a aucun impact sur l'application du Règlement »[1311]. L'extraterritorialité du RGPD constitue une exception au principe de rattachement au territoire de l'Union qui a pour fondement « la souveraineté étatique »[1312] laquelle « s'exerce sur un territoire défini et sur lequel un État est légitime à prendre des mesures de coercition, par le truchement d'autorités de contrôle administratives comme la CNIL en France ou par l'intervention du juge »[1313]. Il en ressort que le caractère extraterritorial et les clarifications apportées par cette disposition sont considérés comme étant « une évolution significative de la législation de l'Union européenne en matière de protection des données par rapport au cadre défini par la directive 95/46/CE[1314] »[1315]. Ce texte, également, vient conforter la position de la Cour de justice de l'Union européenne (CJUE)[1316] et donc renforcer le droit à la réparation des personnes physiques. Cette extension du champ d'application territoriale de la réglementation européenne à des États tiers, par l'article 3, témoigne « l'intention du législateur de garantir une protection complète des droits des personnes concernées dans l'Union (…), dans un contexte de circulation mondiale des données »[1317]. Ces dispositions permettent l'établissement « d'un cadre général de protection des droits de la personnalité, contre des atteintes à ce droit par des responsables du traitement établis en dehors de l'Union européenne »[1318]. Tel qu'affirmé par Madame Thelisson, « Le champ d'application spatial de l'article 3 RGPD s'étend potentiellement au monde entier »[1319].

***550. L'application favorable de la clause relative au droit applicable.*** Dans le cadre d'un contrat de cloud computing entre un client, personne physique, et un prestataire de services cloud, il est très souvent précisé que les données qui sont fournies dans les services cloud peuvent être

[1311] Gallardo Meseguer M., « Aperçu de la dimension internationale du Règlement général sur la protection des données à caractère personnel », in Grosjean A., Enjeux européens et mondiaux de la protection des données personnelles, Bruxelles, Larcier, 2015, p. 117.

[1312] La souveraineté étatique constitue un attribut essentiel de l'Etat permettant de garantir son indépendance (souveraineté politique, juridique et économique), il s'agit d'un statut juridique issu du droit international public : v. article 1er de la Charte des droits et devoirs économiques des États, adoptée par l'assemblée générale des Nations Unies le 12 décembre 1974, « chaque État a le droit souverain et inaliénable de choisir son système économique, de même que ses systèmes politique, social et culturel, conformément à la volonté de son peuple, sans ingérence, pression ou menace extérieure d'aucune sorte » : Assemblée générale des Nations Unies, Résolution 3281, 29e session, 12 décembre 1974.

[1313] CJUE, 5 juin 2018, Witschaftsakademie Schleswig-Holstein, aff. C-210/16, point 52 : Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p. 508, *op. cit.*.

[1314] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[1315] CEPD, Lignes directrices 3/2018 du 12 novembre 2019 relatives au champ d'application territorial du RGPD (article 3).

[1316] CJUE 13 mai 2014 (grande chambre), Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, aff. C-131/12.

[1317] CEPD, Lignes directrices 3/2018 du 12 novembre 2019 relatives au champ d'application territorial du RGPD (article 3).

[1318] Grosjean A., Enjeux européens et mondiaux de la protection des données personnelles, Larcier, 2015, p.85.

[1319] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p. 3, *op. cit.*.

transférées par « des entités du monde entier »[1320]. Il est, donc, intéressant de se poser la question de la loi applicable, à ce contrat de cloud computing, en cas de différend. À ce titre, il est expressément prévu que lorsque les utilisateurs des services cloud sont des citoyens d'un des pays de l'Union européenne, de la Suisse, de la Norvège ou de l'Islande, les lois et la juridiction applicables seront celles du lieu habituel de résidence[1321]. Afin de se mettre en conformité avec le RGPD, le prestataire de service cloud précise qu'il utilise « des clauses contractuelles types approuvées pour le transfert international de renseignements recueillis au sein de l'Espace économique européen et de la Suisse »[1322]. L'intégration de ces clauses contractuelles types permet à la personne physique d'éviter un conflit de lois. Ces clauses permettent à la personne physique de disposer des garanties équivalentes à celles contenues dans le RGPD pour la préservation de son droit à la protection des données et renforcent, ainsi, son droit à réparation en cas d'atteinte.

***551.*** Après avoir étudié le renforcement de la protection des données par l'application extraterritoriale du RGPD, il est envisagé d'étudier l'application extraterritoriale de la compétence juridictionnelle.

## B) Le renforcement de la protection des données par l'application extraterritoriale de la compétence juridictionnelle

***552. La portée extraterritoriale du RGPD en matière de compétence juridictionnelle.*** En raison d'une croissance fulgurante de la mondialisation des échanges des données, l'exécution des contrats cloud suscite inévitablement des questions relatives à la compétence juridictionnelle et pose la problématique « d'une déterritorialisation du droit ». Le RGPD tente d'encadrer la protection des données personnelles dans un contexte international et pour cela permet une application extraterritoriale. Les obligations issus du RGPD d'un État membre s'étendent non seulement sur des faits situés dans un autre État membre, mais en dehors de l'Union européenne. Ce texte a, donc, une application extraterritoriale et constitue une dérogation au principe de souveraineté étatique[1323]. En effet, le caractère extraterritorial du texte est contraire

[1320] Contrat I.cloud de la société Apple : https://www.apple.com/legal/privacy/fr-ca/.

[1321] Ibid.

[1322] Ibid.

[1323] V. article 1er de la Charte des droits et devoirs économiques des États, adoptée par l'assemblée générale des Nations Unies le 12 décembre 1974 et Résolution 3281 de l'Assemblée générale des Nations Unies, 29e session, 12 décembre 1974.

au principe de la compétence territoriale issu du droit international public[1324]. Le risque, ici, est l'existence d'un conflit de lois, lequel pourrait déboucher lui-même sur un conflit de juridiction. Il est possible pour des faits découlant de l'exécution d'un contrat, des juridictions émanant d'États différents se déclarent être compétentes. Pour sécuriser la protection des données personnelles sur le territoire de l'Union européenne, l'objectif serait d'attribuer la compétence juridictionnelle exclusive à un État membre de l'Union européenne. Cette attribution de compétence juridictionnelle permettrait d'appliquer la réglementation européenne protectrice des données personnelles (en particulier, le RGPD) et éviter « le risque de la double peine, qui serait contraire au principe *non bis in idem* ? »[1325].

***553.*** Si chaque État dispose d'une souveraineté étatique, comment permettre l'extension de la compétence juridictionnelle pour des faits situés hors de l'Union européenne ? Sans contrevenir au principe de souveraineté étatique et donc du principe de compétence territoriale des États, l'une des voix avancées est de considérer que le droit à la protection des données est un droit fondamental[1326] qui vise la protection de la personne humaine et « les droits de l'homme ont une prétention à l'universalité »[1327]; en conséquence « l'Union pourrait appliquer le RGPD de manière universelle, sur la base d'une infraction à la protection des données en tant que violation d'un droit humain fondamental »[1328]. Si l'Union européenne est favorable à l'application des principes d'universalités des droits fondamentaux, « cette conception n'est cependant pas partagée sur la scène internationale et il n'est pas exclu que certains pays comme la Chine ou les États-Unis s'opposent à cette reconnaissance »[1329]. Face à une situation de blocage diplomatique, l'issue de sortie serait sans doute la conclusion d'accord bilatéral ou multilatéral en matière de compétence juridictionnelle pour les litiges relatifs au traitement de données personnelles. D'autres auteurs ont proposé « la création de nouveaux territoires de la taille du réseau internet »[1330] ; également, « la création d'un espace d'échange de données a-territorial a émergé de manière concomitante avec les mécanismes de *soft law »*[1331].

---

[1324] Il s'agit d'un principe qui donne compétence à l'État à l'égard des biens et des personnes situés sur son territoire et des situations rencontrées sur ce même territoire : v. art. 2, § 1 de la charte des Nations Unies du 26 juin 1945, lequel reconnaît le principe d'égalité souveraine de tous les États membres. Il s'agit, « En théorie, les États souverains sont donc tous égaux, quelles que soient leur superficie, leur population et leur puissance réelle » : Actes & Colloques, Le principe de l'article 2 § 1 de la Charte des Nations Unies, Entre théorie et pratique, Faculté de droit et des sciences sociales de Poitiers, 14 janvier 2014.

[1325] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p. 512, *op. cit.*.

[1326] Art. 8 paragraphe 1 de la Charte des Droit Fondamentaux de l'Union Européenne.

[1327] V. Déclaration universelle des droits de l'homme du 10 décembre 1948, en particulier art.2 § 2.

[1328] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p. 514, *op. cit.*.

[1329] Ibid.

[1330] Johnson D.R, D. Post, « Law and Borders – The Rise of Law in Cyberspace », Stan. L. Rev., 1995, vol. 48, p. 1367, in Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p.514, *op. cit.*.

[1331] V. Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p. 514, *op. cit.*. V. également, Schmid Ch., Nadakavukaren Schefer K. et Heckendorn Urscheler L., Conflict of laws in the maze of digital platforms -

***554. La résolution des conflits de lois en matière de compétence juridictionnelle***. Il apparaît qu'en matière de protection des données personnelles, le RGPD permet de limiter « le recours à la règle de conflit de lois au sein de l'UE »[1332] puisque ce texte harmonise entre les États membres le niveau de protection des données. En revanche, la règle de conflit de lois réapparaît lorsqu'il s'agit de pays tiers à l'Union européenne. Une juridiction d'un État tiers à l'Union européenne pourrait être saisie dans le cadre d'un recours relatif à la protection des données personnelles. Cela signifie qu'il peut exister une concurrence de juridiction qui fait naître une insécurité juridique en lien avec l'autorité de la chose jugée (*res iudicata*) et la règle *non bis in idem*.

***555.*** À l'instar du droit applicable, le RGPD a apporté des clarifications en matière de compétence juridictionnelle afin de rendre effectif le droit à réparation des personnes physiques en cas d'atteinte au droit à la protection des données personnelles. À ce titre, pour déterminer le tribunal territorialement compétent, l'article 79 du RGPD précise que l'action devra être intentée devant les juridictions de l'État membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement ou devant les juridictions de l'État membre dans lequel la personne concernée a sa résidence habituelle. Cette disposition met en œuvre le critère de la localisation du responsable du traitement ou du sous-traitant ou de la personne physique concernée par le traitement. Afin de limiter le recours de la règle de conflit de lois lorsqu'il s'agit d'un État tiers à l'Union, il est proposé de lire cette disposition en lien avec l'article 3 du RGPD qui traite du champ d'application territoriale du règlement. Par cette lecture, l'idée est d'attribuer la compétence juridictionnelle à un tribunal dans un État de l'Union européenne où se situe le sous-traitant ou la personne physique alors même que le responsable du traitement se trouve dans un État tiers. Dès lors que les conditions de l'article 3, al. 2, du RGPD sont remplies, la compétence juridictionnelle devrait être attribuée à un tribunal au sein de l'Union européenne.

***556.*** Mais au regard du principe de souveraineté étatique, certains États peuvent s'interroger sur la licéité et l'applicabilité du RGPD sur leur territoire. Il peut exister une divergence entre les États-Unis et l'Union européenne quant à l'applicabilité de leur texte ayant une portée extraterritoriale, laquelle engendre un conflit de juridiction. En effet, « le RGPD et le *Cloud Act* ont le potentiel pour créer des interférences dans les relations internationales du fait du rôle

---

Le droit international privé dans le labyrinthe des plateformes digitales : actes de la 30e Journée de droit international privé du 28 juin 2018 à Lausanne, n°86, L'Institut suisse de droit comparé, Edition Romandes Schulthess, 2018.

[1332] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p. 518, *op. cit.*.

stratégique des données dans l'économie et la politique des États »[1333] et « témoigne d'une approche extensive du principe de souveraineté »[1334]. À titre illustratif, « l'intervention d'un gouvernement étranger dans une procédure privée est perçue aux États-Unis comme une atteinte aux droits des parties et à l'indépendance du pouvoir judiciaire reconnue par la Constitution »[1335]. En effet, l'applicabilité du RGPD dans un État tiers à L'Union européenne soulève la question de la conformité des prescriptions de ce texte avec les lois en vigueur dans l'État tiers. En raison des difficultés liées à la résolution des conflits de lois et de juridictions, des voix s'élèvent pour la reconnaissance d'une juridiction pour « le cyberespace »[1336].

***557.*** La volonté d'un renforcement de la protection des données en matière de cloud computing soulève le problème de la territorialité en matière de compétence juridictionnelle. La « territorialité » permet à un État d'exercer sa souveraineté, mais « le concept de souveraineté n'exige pas toujours que la juridiction soit fondée sur la territorialité, uniquement »[1337]. En effet, il existe des exceptions au principe de territorialité fondées sur un droit d'ordre public telles que les réglementations applicables aux ressortissants d'un État situé dans un État tiers. Face à ce constat, la doctrine considère que « la juridiction en tant que concept jurisprudentiel n'est pas enracinée dans la territorialité »[1338] ». Est-ce qu'il ne s'agirait pas, plutôt, aujourd'hui, de se tourner vers une juridiction spécifique détachée de tout territoire [1339]. Il s'agirait de concevoir une juridiction qui serait rattachée non pas à un territoire terrestre, mais à un nouvel espace de circulation des données personnelles. Le RGPD a intégré cette spécificité en proposant un cadre pour régir cet espace de circulation des données en abandonnant « en partie, l'objectif de localisation de l'activité de traitement »[1340]. Certains auteurs soulignent que l'effectivité du

---

[1333] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p.525, *op. cit.*.

[1334] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p.526, *op. cit.*.

[1335] Neale A.D et Stephens M.L., International Business and National Jurisdiction, 1re éd., Oxford, Clarendon Press, 1988, pp. 30 ss.

[1336] McLachlan C., « From Savigny to Cyberspace: Does the Internet Sound the Death-Knell for the Conflict of Laws? », Media and Arts Law Review, 2006, vol. 11, p. 418. V. Delmas-Marty M., Vers une communauté de valeurs ? Les forces imaginantes du droit (IV), Paris, Seuil, 2011, p. 45. Également, v. Bergé J.-S. et Grumbach S., « La sphère des données et le droit : nouvel espace, nouveaux rapports aux territoires », JDI, 2016, p. 1157.

[1337] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données p.527, *op. cit.*.

[1338] Lessig L., « The Law of the Horse: What Cyber Law Might Teach », Harvard Law Review, 1999, vol. 113, p. 506.

[1339] V. *supra* n° 549 (juridiction d'un cyberespace). Également, v. Ettighoffer D.-C., L'économique numérique sera-t-elle sous domination américaine ? Géoéconomie 2010/2 (n° 53), pages 89 à 99 : « La société française voit l'ensemble des référentiels géostratégiques et socio-économiques bouleversé par l'importante croissance de l'économie immatérielle, par la numérisation du monde et par la prolifération des réseaux. Alors que cette numérisation affecte les fonctions de production, de l'éducation, de la recherche, du commerce et de la distribution, saurons-nous maîtriser les infrastructures qui irriguent l'économie numérique alors que se profilent les développements prometteurs des applications du grid computing et du cloud computing ? Serons-nous une nation stratège dans ce nouveau monde de l'économie numérique alors que nous sommes loin de maîtriser les voies de navigation modernes du cyberespace ?(…) La globalisation numérique recouvre un monde socio-économique multipolaire bien déterminé à utiliser les réseaux électroniques pour se cultiver et s'enrichir. Autrefois, pour ce faire, on devait s'insérer dans les circuits commerciaux des biens.Face à l'enjeu majeur que représente la maîtrise des infrastructures qui maillent l'économie du futur, le fait que les Américains gouvernent Internet est moins la preuve de leur force que celle de notre propre faiblesse » : https://www.cairn.info/revue-geoeconomie-2010-2-page-89.htm.

[1340] Bergé J.-S. et Grumbach S., « La sphère des données et le droit : nouvel espace, nouveaux rapports aux territoires », JDI, 2016, pp. 1153-1173. Egalement, v. les jurisprudences relatives à une interprétation extension extensive du critère d'application territorial

RGPD « dépend de la capacité de l'Union européenne à en assurer la prévalence sur les ordres publics des États tiers »[1341], en particulier sur les États-Unis.Tel que préconisé par certains auteurs, il serait opportun pour l'Union européenne « d'adopter, via des conventions internationales, des mesures permettant d'assurer une prééminence réelle de la règle européenne en matière de protection des données sur les ordres publics étrangers »[1342].

***558.*** Afin de garantir un niveau élevé de protection aux personnes privées sur le plan mondial et d'apporter une réponse à la « déterritorialisation du droit », des auteurs[1343] proposent un droit mondial de la protection des données sur le modèle de la Convention 108 du Conseil de l'Europe[1344]. Il s'agirait d'élaborer « un code mondial du droit de la protection des données, harmonisant les droits nationaux en ce domaine » permettant de « résoudre les conflits de juridictions résultant de l'application du droit de la protection des données »[1345]. Malgré la pertinence théorique de cette proposition, il est considéré que celle-ci ne pourrait prospérer « tant les conceptions sur la nature de la donnée (bien marchand ou attribut de la personnalité protégé en tant que droit fondamental) varient d'un État à l'autre »[1346].

***559.*** Si l'élaboration d'un droit mondial de la protection des données semble pour certains constituer une solution peu réaliste, il convient de se tourner vers le contrat afin de prévoir une protection juridictionnelle effective. Il serait opportun de responsabiliser les prestataires de services cloud d'intégrer dans les contrats cloud une clause attribuant la compétence juridictionnelle à un tribunal situé sur le territoire européen dès lors qu'il s'agit de données personnelles de personnes physiques situés dans l'Union européenne. Il s'agirait, en réalité, de traduire par convention la règle défendue par le RGPD découlant de la combinaison des articles 3 et 79.

---

de la protection européenne des données personnelles, en dehors de l'Union dès lors qu'il existe dans l'Union une succursale (affaire Google Spain, CJUE, 13 mai 2014, affaire n° C-131/12, Google Spain SL, Google Inc. c/ Agencia Española de Protección de Datos (AEPD) et Mario Costeja González) ou un représentant du responsable du traitement (affaire Google Weltimmo, CJUE, 1er octobre 2015, affaire n° C-230/14, Weltimmo), afin d'assurer une protection effective du droit à la protection des données personnelles.

[1341] Deroudille A. et Fatah. F., « L'extraterritorialité du RGPD dans le contexte du Cloud Act », RUE, 2019, p. 442.

[1342] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p. 530, *op. cit.*.

[1343] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p.532, *op. cit.*.

[1344] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28.01.1981, Art.1 : Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant («protection des données») ». Ouverte à la signature depuis le 28 janvier 1981, il s'agit du premier instrument international juridique contraignant dans le domaine de la protection des données. Aux termes de cette Convention, les parties doivent prendre les mesures nécessaires en droit interne pour en appliquer les principes afin d'assurer, sur leur territoire, le respect des droits fondamentaux de la personne humaine au regard de l'application de la protection des données.

[1345] Thelisson E., La portée du caractère extraterritorial du Règlement général sur la protection des données, p.532, *op. cit.*.

[1346] Ibid.

***560. L'application favorable de la clause relative à la compétence juridictionnelle.*** Lorsque le contrat cloud est conclu entre un prestataire de services cloud et un consommateur résidant dans l'Espace économique européen ou en Suisse, le contrat précise que « tout litige qui résulte des présentes conditions ou qui est lié à ces dernières est régi par le droit et les tribunaux de votre pays »[1347]. Par cette disposition, le droit applicable et la compétence juridictionnelle sont attribués au pays du lieu de résidence de la personne physique. Dès lors que le client est une personne physique résidant dans l'Espace économique européen, nous assistons à l'application des droits issus du RGPD et des lois nationales, lesquels pourront être revendiqués par la victime devant les tribunaux français. Il apparaît que le droit à réparation des personnes physiques est renforcé, ici, par l'application des clauses mentionnant l'application du droit européen et l'attribution de la compétence juridictionnelle à un tribunal d'un État membre de l'Union européenne.

***561.*** Il en résulte de cette analyse contractuelle, que le droit à la protection des données à caractère personnel s'en trouve renforcé[1348], dans un contexte international, dès lors que le contrat de cloud computing prévoit des dispositions contractuelles assurant aux personnes physiques (résidents de l'Union européenne) que le droit applicable et la compétence juridictionnelle sont ceux du lieu habituel de résidence de la personne concernée (donc de l'Union européenne).

[1347] Conditions d'utilisation du service cloud de Google : https ://policies.google.com/terms. Pour comparaison, s'il s'agit d'un utilisateur professionnel dans l'Espace économique européen ou en Suisse, il est précisé que « les présentes conditions sont régies par le droit anglais. Google et vous-même vous soumettez à la juridiction exclusive des tribunaux anglais pour tout litige qui résulte des présentes conditions ou qui est lié à ces dernières ».

[1348] À l'exception de la situation envisagée en première partie, lorsque les États-Unis décident de mettre en œuvre les lois sécuritaires : v. supra n° 208 et suivants.

# Conclusion chapitre 2

***562. Le renforcement de la protection des données à caractère personnel par un élargissement des responsabilités dans un contexte européen.*** Au sein de l'Union européenne, le renforcement de la protection des données dans les contrats cloud est rendu possible grâce à un élargissement du champ des actions en responsabilité. Ces actions en responsabilité sont fondées sur l'atteinte au droit à l'autodétermination informationnelle, sur l'atteinte au droit à la vie privée ainsi que sur des manquements contractuels. Ces fondements juridiques ouvrent la voie, à la personne physique d'une pluralité d'actions en responsabilité exercées à titre individuel ou collectif (action de groupe). Cette pluralité d'actions permet d'engager, séparément ou conjointement, la responsabilité du prestataire de services cloud et de son sous-traitant. L'élargissement des responsabilités et l'inversion de la charge de la preuve au profit du client, personne physique, permettent de renforcer l'effectivité du droit à réparation. Cette effectivité est renforcée par l'admission d'une réparation étendue des préjudices en découlant et par la diversité des sanctions (administratives, civile et pénales). La réparation en cas d'atteinte au droit à l'autodétermination informationnelle est étendue à la réparation du préjudice matériel et moral. En cas d'atteinte au droit à la vie privée, la réparation est même rendue possible en l'absence de préjudice.

***563. Le renforcement de la protection des données à caractère personnel par un élargissement des responsabilités dans un contexte international.*** Par ailleurs, la protection des données est renforcée dans un contexte international par l'application extraterritoriale du droit de l'Union européenne et de la compétence juridictionnelle au profit d'un état membre de l'Union européenne. L'applicabilité de la réglementation européenne hors des frontières de l'Union européenne permet aux clients, personnes physiques, d'agir contre des responsables (le prestataire de services cloud et son sous-traitant) établis hors des frontières de l'Union européenne. La portée extraterritoriale du RGPD en matière de droit applicable permet d'étendre la protection aux personnes situées dans l'UE dont les données sont traitées, et ce indépendamment de la localisation effective du traitement. Il s'agit, donc, d'une protection élargie à toutes les personnes concernées qui se trouvent dans l'Union européenne. Également, la portée extraterritoriale du RGPD ainsi que les prévisions contractuelles en matière de compétence juridictionnelle permettent d'attribuer la compétence juridictionnelle à un tribunal dans un État de l'Union européenne où se situe le sous-traitant ou la personne physique alors même que le responsable du traitement se trouve dans un État tiers. Il en résulte que le droit à réparation des personnes physiques est renforcé dans un contexte international par l'application

extraterritoriale du RGPD et les prévisions contractuelles en matière de droit applicable et de compétence juridictionnelle.

# Conclusion du Titre 1

***564. La quête du renforcement de la protection des données.*** Cette partie a étudié les mesures palliatives applicables au renforcement de la protection des données personnelles des personnes physiques dans les contrats de cloud computing. Il en est ressorti que la protection des données à caractère personnel dans les contrats de cloud computing est renforcée par la mise en œuvre de droits liés à la titularité des données et le droit à la réparation.

***565. Le renforcement de la protection par les droits liés à la titularité des données.*** Après avoir considéré l'inadaptation du concept de propriété à la protection des données dans les contrats de cloud computing au regard des exigences du droit positif, l'étude s'est tournée en faveur d'une mise en œuvre de la théorie personnaliste du droit à la protection des données. L'attention a, donc, été portée sur le développement d'autres droits spécifiques à la protection des données et en particulier le droit à l'autodétermination informationnelle. Il résulte de cette étude que c'est grâce à la consécration dans les textes de ce droit à l'autodétermination accompagné de ses prérogatives et l'intégration de ces principes légaux dans le contrat cloud que la protection des données personnelles s'en trouve renforcée.

***566. Le renforcement de la protection des données à caractère personnel dans les contrats de cloud computing par le droit à réparation.*** Dans cette partie, la réflexion du renforcement de la protection des données à caractère personnel dans les contrats de cloud computing par le droit à réparation a été menée autour du renforcement d'un élargissement du champ des actions en responsabilité dans un contexte européen et international. C'est en raison de l'élargissement des actions en responsabilités, l'admission d'une réparation étendue et d'une diversité des sanctions que le droit à la réparation est renforcé en Union européenne. Pour rendre effective la protection des données personnelles, dont bénéficient les personnes physiques au niveau de l'Union européenne, il paraissait fondamental de pouvoir prétendre à une application extraterritoriale de la réglementation européenne. Le droit de l'Union européenne de la protection des données personnelles a une application extraterritoriale laquelle permet aux personnes physiques d'exercer une action en responsabilité à l'encontre d'un prestataire de services cloud et son sous-traitant établis hors des frontières de l'Union européenne et de bénéficier d'une compétence juridictionnelle européenne. Cette étude a mis en lumière que l'application extraterritoriale du RGPD ainsi que les prévisions contractuelles concernant le droit applicable et la compétence juridictionnelle permettent d'étendre de manière effective la protection des

données personnelles des personnes physiques situées dans l'Union européenne et ce peu importe si le traitement des données est localisé en dehors de l'Union européenne.

***567.*** Après avoir étudié le renforcement de la protection des données à caractère personnel des personnes physiques, il est envisagé d'étudier le renforcement de la protection des données numériques des personnes morales dans le cloud computing.

# Titre 2 : Les renforcements de la protection des données des personnes morales dans les contrats de cloud computing

***568. Les moyens juridiques et contractuels.*** À ce jour, il n'existe pas de texte spécifique à la protection des données confidentielles des personnes morales équivalent à celui consacré à la protection des données à caractère personnel, tel que le RGPD[1349]; en revanche, il existe des réglementations particulières en fonction de la nature de la donnée concernée[1350]. Aujourd'hui, la protection des données des personnes morales est assurée par des outils juridiques tels que l'adaptation de certaines réglementations en vigueur[1351] et par la technique contractuelle.

***569. Le renforcement par la loi.*** Cette étude est entreprise à travers la notion du « patrimoine informationnel » et du régime des responsabilités. Il est procédé à l'étude du cadre légal du patrimoine informationnel afin d'identifier les moyens juridiques permettant de contribuer au renforcement de la protection des données. En particulier, il est envisagé d'étudier le droit de la propriété intellectuelle et industrielle et le droit commun des affaires.

***570. Le renforcement par le contrat.*** En outre, la personne morale doit veiller à l'insertion dans le contrat de cloud computing de clauses spécifiques pour renforcer la protection de ses données. Pour appréhender la question de la sécurisation contractuelle quant à la protection des données des personnes morales, il est envisagé d'étudier de manière spécifique les clauses relatives à la sécurité technique et à la sécurité juridique. Concernant l'étude des clauses relatives à la sécurité technique, il est procédé à l'analyse des clauses qui traitent de la sécurité de l'infrastructure et en particulier celles qui concernent les mesures techniques (les sauvegardes, les contrôles d'accès, le chiffrement) ainsi que la clause relative à la réversibilité des données (ou du droit de portage). S'agissant des clauses relatives à la sécurité juridique, il s'agit d'étudier les clauses du contrat cloud qui permettent de prémunir le client, personne morale, d'un risque juridique quant à une éventuelle atteinte à ses données stockées dans le cloud ; en particulier, les clauses relatives à la confidentialité et à l'interdiction de l'exploitation des données.

---

[1349] Considérant 14 du RGPD : « Le présent règlement ne couvre pas le traitement des données à caractère personnel qui concernent les personnes morales, et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale ».

[1350] V. *infra* n° 575.

[1351] Aujourd'hui, au niveau de l'Union européenne, les enjeux du cloud computing et du marché de la « donnéé » sont intégrés dans les nouveaux textes : le Règlement (UE) 2022/868 du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), le Règlement (UE) 2022/1925 du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques ou DMA), le Règlement (UE) relatif à un marché intérieur des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques ou DSA) adopté le 4 octobre 2022.

***571.*** **Plan du Titre 2** : Cette partie est consacrée à l'étude du renforcement de la protection des données de la personne morale par la loi (Chapitre 1) et par le contrat (Chapitre 2).

# Chapitre 1 : Le renforcement de la protection des données par la loi

***572.*** ***Le renforcement de la protection des données des personnes morales par la notion du patrimoine informationnel***. Aujourd'hui, la valeur financière d'une entreprise se mesure non seulement par ses éléments corporels (stocks, matériels d'exploitation), mais également par ses actifs immatériels, telle que les informations dont elle détient concernant l'état du marché, de la concurrence, des informations relatives aux fournisseurs et aux clients, des données stratégiques (..). C'est afin de renforcer la protection des données confidentielles de la personne morale de droit privé que la notion de « patrimoine informationnel » est apparue. L'étude s'intéresse, ainsi, à la protection dans les contrats de cloud computing de ces données regroupées sous la notion de patrimoine informationnel**.** Dans la pratique, il apparaît que les personnes morales se posent la question du renforcement de la protection de leur patrimoine informationnel quand elles concluent un contrat de cloud computing. À cette question, il est envisagé d'étudier quel est le cadre légal attaché à la protection du patrimoine informationnel en fonction de la donnée concernée et quels sont les moyens juridiques attachés à cette protection.

***573.*** ***Plan***. Il est fait le choix d'étudier distinctement le renforcement de la protection des données des personnes morales par le droit de la propriété intellectuelle et industrielle (**Section 1**) et par le droit commun des affaires (**Section 2**).

## Section 1 : Le renforcement de la protection des données par le droit de la propriété intellectuelle et industrielle

***574.*** Certaines données confidentielles de la personne morale ont pu être protégées, en droit de la propriété intellectuelle et industrielle, par le concept d'un secret spécifique et de droits spécifiques.

***575.*** ***Plan.*** Il est envisagé d'étudier, dans cette partie, le renforcement de la protection des données confidentielles de la personne morale par un « secret » spécifique (A) et des droits spécifiques (B).

## A) La protection du patrimoine informationnel par un secret spécifique

***576.*** La protection par le « secret » spécifique en droit de la propriété intellectuelle et industrielle porte sur certaines données précises composant le patrimoine informationnel.

***577.*** ***Plan.*** Avant d'envisager l'étude de la protection de ces données par le « secret » spécifique (2), il est procédé, tout d'abord, à l'étude de la détermination du patrimoine informationnel (1).

### 1) La détermination du patrimoine informationnel

***578.*** ***La patrimoine informationnel, un outil juridique.*** Aujourd'hui, les personnes morales revendiquent une protection proche de celle reconnue aux personnes physiques sur leurs données personnelles. Il s'agirait de revendiquer une forme de protection de la vie privée des entreprises. Nous assistons ces dernières années à une volonté de rapprochement du droit des données des personnes physiques et des personnes morales. En effet, les personnes physiques aspirent à la reconnaissance de droits patrimoniaux sur leurs données tandis que les personnes morales plébiscitent un renforcement de la protection de leur patrimoine informationnel. La protection demandée porte précisément sur ce que l'on appelle *le patrimoine informationnel* de l'entreprise. Le concept de *patrimoine informationnel* est appréhendé comme un outil juridique au profit des personnes morales pour renforcer la protection de leurs données confidentielles.

***579.*** ***La définition de la notion de « patrimoine informationnel », au niveau national.*** Ce patrimoine informationnel a été défini par la pratique, en France, comme étant « l'ensemble des données, protégées ou non, valorisables ou historiques, d'une personne physique ou morale »[1352] disposant « d'une valeur économique ou un intérêt stratégique, indépendamment du caractère protégeable ou non de ces informations par un droit de propriété intellectuelle »[1353]. Le patrimoine informationnel correspond, ainsi, à « l'universalité des données détenues et produites par une personne physique ou morale, composante de son patrimoine immatériel. Il s'agit, donc, d'un ensemble de droits et de devoirs, d'actifs et de passifs, en mutation permanente en fonction des

[1352] Livre blanc du CIGREF (Club informatique des grandes entreprises françaises), en partenariat avec la FedISA (Fédération de l'ILM, du stockage et de l'archivage), Protection du patrimoine informationnel, publié le 30 novembre 2007, définition du patrimoine informationnel.

[1353] Galloux J.-C. « Ebauche d'une définition juridique de l'information », 1994, Dalloz chronique pp. 229-234.

événements juridiques de la vie numérique d'une donnée »[1354]. Cette notion correspondrait comme l'affirment certains auteurs à « une autre universalité de fait, constituée de secrets d'affaires de toute nature »[1355]; d'un patrimoine *sui generis*, constitué de biens meubles incorporels. Le patrimoine informationnel est composé, ainsi, de diverses données et constitue l'actif immatériel de l'entreprise.

***580. La définition de la notion de « patrimoine informationnel », au niveau international.*** La notion de « patrimoine informationnel » a, également, été appréhendée par le droit international comme étant des renseignements licitement sous le contrôle des personnes morales qui ont un caractère secret et disposant d'une valeur commerciale[1356]. Au niveau européen, le patrimoine numérique informationnel a été défini, à l'article 1er du règlement d'exemption européen du 27 avril 2004, sous l'angle du « savoir-faire » comme « un ensemble d'informations pratiques non brevetées, résultant de l'expérience et testées » lequel est soumis à trois critères cumulatifs : il doit être substantiel, il doit être identifié et il doit être secret »[1357]. Le caractère substantiel signifie qu'il soit important et utile pour la production des produits contractuels. Le caractère identifié correspond à l'idée qu'il doit être décrit d'une façon suffisamment complète pour permettre de vérifier que les conditions de secret et de substantialité sont remplies. Quant au caractère secret qui se rattache à l'exigence que la donnée concernée ne doit pas être connu ou facilement accessible par des tiers. En droit international et en droit de l'Union européenne, le critère commun, pour déterminer le patrimoine informationnel, est le caractère secret. En effet, c'est parce que la donnée est « secrète » qu'il est demandé une protection légale contre toute la divulgation. En pratique, les données à protéger correspondent aux données se rapportant, ainsi, aux analyses de marché, de marketing, de stratégies commerciales, aux bases de données clients et fournisseurs, au savoir-faire de l'entreprise (..)[1358]. Ces informations constituent ce que l'on appelle l'actif immatériel de l'entreprise et dispose, à ce titre, d'une forte valeur financière qu'il faut protéger[1359] d'autant plus que la personne morale recourt à la technologie du cloud pour héberger lesdites données. Il est,

[1354] Saint-Aubin Th., les nouveaux enjeux juridiques des données (big data, web sémantique et linked data) Les droits de l'opérateur de données sur son patrimoine numérique informationnel, Revue Lamy Droit de l'Immatériel, Nº 102, 1er mars 2014.

[1355] De Maison Rouge O., « Le patrimoine informationnel : fonds de commerce du XXIème siècle ? 6 mai 2010, https://www.village-justice.com/articles/spip.php?page=imprimer&id_article=7827.

[1356] Art. 39.2, accord ADPIC (Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce).

[1357] Règlement d'exemption européen 772/2004 du 27 avril 2004 relatif aux accords commerciaux, définition du patrimoine informationnel donnée par l'article 1 reprenant les termes du règlement CEE n°4087/88 du 30 novembre 1988.

[1358] Livre blanc du CIGREF (Club informatique des grandes entreprises françaises), en partenariat avec la FedISA (Fédération de l'ILM, du stockage et de l'archivage), Protection du patrimoine informationnel, publié le 30 novembre 2007, définition du patrimoine informationnel.

[1359] Ibid.

donc, question d'étudier comment la mise en œuvre de ce concept permet de renforcer la protection des données des personnes morales dans les contrats de cloud computing.

***581. L'application de régimes distincts en fonction du type de donnée.*** Outre la nécessité de concevoir une sécurité des systèmes d'informations fiables[1360], le client, personne morale, doit s'assurer que son patrimoine informationnel est, également, efficacement protégé[1361] lorsqu'elle conclut un contrat de cloud computing. C'est dans un souci, ainsi, de protection des données des personnes morales que la notion de « patrimoine informationnel » a vu le jour et a été utilisée initialement pour justifier l'exploitation de droits exclusifs[1362]. À l'intérieur de cette universalité (patrimoine informationnel), il est possible d'observer que le régime juridique applicable pour chaque donnée s'articule autour des droits d'usage, des droits d'exploitation et des obligations de conservation sur ce patrimoine informationnel numérique[1363]. Pour appréhender le régime de protection du patrimoine informationnel, il s'agit de procéder à l'intérieur de cette universalité à une « catégorisation juridique des données »[1364] laquelle passe par le recensement de variables permettant de déterminer les règles applicables à chacune de ces catégories de données.

***582. La catégorisation des données composant le patrimoine informationnel.*** Chacune des catégories de données qui composent ce patrimoine informationnel numérique de l'entreprise pourront, ainsi, être protégée par des réglementations particulières telles que la propriété intellectuelle et industrielle avec l'application d'un secret spécifique, du droit d'auteur, le droit des bases de données, le droit des brevets, le droit des marques, le droit des dessins et modèles, la protection du savoir-faire, la protection du secret de fabrique, la protection des signes distinctifs (nom commercial, enseigne, dénomination sociale, nom de domaine) et les mesures techniques de protection et d'information[1365]. Le renforcement de la protection du patrimoine informationnel réside, ici, dans l'application de ces régimes juridiques spécifiques.

---

[1360] Livre blanc du CIGREF -FedISA, Protection du patrimoine informationnel, 30 novembre 2007.

[1361] Hagel F. « Secret et droits de propriété intellectuelle : un tour d'horizon », Revue Lamy de l'immatériel 10/2009, n°53.

[1362] Saint-Aubin Th., les nouveaux enjeux juridiques des données (big data, web sémantique et linked data) Les droits de l'opérateur de données sur son patrimoine numérique informationnel, Revue Lamy Droit de l'Immatériel, N° 102, 1er mars 2014.

[1363] Ibid.

[1364] Ibid.

[1365] Bensoussan A., le Patrimoine informationnel de l'entreprise : https://www.alain-bensoussan.com/avocats/la-protection-du-patrimoine-informationnel-de-l'entreprise/2010/03/09/.

***583.*** Il est, donc, proposé d'étudier, dans la partie suivante, le « secret » spécifique en droit de la propriété intellectuelle et industrielle afin de renforcer la protection de certaines données du patrimoine informationnel dans le cadre de l'exécution d'un contrat de cloud computing.

**2) La protection par un secret spécifique**

***584.*** La protection d'un secret spécifique correspond, ici, à la protection du savoir-faire et le secret de fabrication de la personne morale. Il s'agit d'une protection accordée de manière spécifique par le droit de la propriété intellectuelle et industrielle à certains types de données spécifiques et non à l'ensemble des données confidentielles des personnes morales composant le patrimoine informationnel.

***585.*** ***Plan***. Dans cette partie, il est envisagé d'étudier distinctement la protection par le savoir-faire (a) et le secret de fabrique (b).

a) La protection par le savoir-faire

***586.*** ***La détermination du savoir-faire***. Lorsque la personne morale conclut un contrat de cloud computing avec un prestataire de services cloud, elle héberge dans l'infrastructure cloud son patrimoine informationnel ce qui inclut les données relatives au savoir-faire. Juridiquement, le savoir-faire est défini comme étant « un ensemble d'informations pratiques non breveté, résultant de l'expérience et testé, qui est secret (..), substantiel(..), identifié (..) »[1366]. Le caractère *secret* signifie que l'information concernée « n'est pas généralement connue ou facilement accessible »[1367]. Le caractère *substantiel* se rapporte à l'importance et l'utilité de l'information concernée pour la production des produits contractuels[1368]. Quant au caractère *identifié, il* correspond à l'idée que l'information concernée doit être décrite d'une façon suffisamment complète pour permettre de vérifier que les conditions de secret et de substantialité sont remplies[1369]. Au niveau de la doctrine, la définition du savoir-faire communément retenue est celle du Professeur Jean-Marc Mousseron qui le définit comme étant une « connaissance technique transmissible, mais non immédiatement accessible au public et non brevetée »[1370]. Le savoir-faire constitue, alors, « un ensemble d'éléments qui sont le fruit de l'expérience et constituent une avancée technologique

[1366] V. art. 1er du règlement d'exemption n° 772/2004 du 27 avril 2004.

[1367] Ibid.

[1368] Ibid.

[1369] Ibid.

[1370] Mousseron M., Secret et contrats – de la fin de l'un à la fin de l'autre –, Mélanges Foyer, 1997, PUF, p. 257.

commerciale »[1371]. Pour reprendre les caractéristiques du savoir-faire, il doit pouvoir être transmissible[1372], que la connaissance ne doit pas être immédiatement accessible au public et revêtir un caractère technique, non inventif, non breveté, secret et substantiel. En contractualisant avec un prestataire de services cloud une offre d'hébergement dans un cloud computing, le client, personne morale, va utiliser cette infrastructure pour conserver ses données de savoir-faire. Étant dans le nuage, la question de la protection de ce savoir-faire se pose en cas d'atteinte à ces données par le prestataire de services cloud.

***587. La protection du savoir-faire par le contrat cloud.*** À ce jour, le savoir-faire ne fait pas l'objet d'un droit privatif au profit de son détenteur, il ne peut, donc, exercer aucun monopole sur ce savoir-faire. Pour protéger la donnée stockée dans le cloud computing, renfermant un savoir-faire, le client, personne morale, doit recourir à la protection contractuelle. À titre illustratif, en dépit que le savoir-faire n'accorde aucun droit privatif à la personne morale, il est possible par convention d'indiquer que cette dernière demeure propriétaire des données relatives à son savoir-faire. En effet, le détenteur du secret n'a pas de droit de propriété (au sens juridique du terme) sur les informations non protégées par un titre de propriété intellectuelle ou industrielle (brevet, marque, droit d'auteur, dessins et modèles), mais le contrat peut indiquer une propriété au sens commun du terme désignant que le détenteur exerce, de manière exclusive, des prérogatives sur ses données couvertes par le secret. Cette protection conventionnelle peut être contenue directement dans le contrat de cloud computing au travers de clauses spécifiques telles que la clause relative à « l'obligation du Prestataire de non-accès, de non-traitement et de non-exploitation des données relatives au savoir-faire du Client » ou bien figurer dans un acte annexé au contrat de cloud computing, tel qu'un accord de confidentialité. Il est proposé ci-après une proposition de rédaction de cette clause relative à « l'obligation du Prestataire de non-accès, de non-traitement et de non-exploitation des données relatives au savoir-faire du Client » :

« Dans le cadre des présentes, le Client n'accorde au profit du Prestataire aucune licence d'exploitation de son savoir-faire hébergé dans l'infrastructure cloud du Prestataire. Le savoir-faire du Client est entendu, ici, largement et de manière non limitative comme étant « un ensemble d'informations pratiques non breveté, résultant de l'expérience et testé, qui est secret, substantiel et identifié » (art. 1er du règlement d'exemption n° 772/2004 du 27 avril 2004). Il est entendu que les informations couvertes par le savoir-faire (ci-après désignées « Savoir-faire ») sont protégées par les présentes et incluent de manière non limitative, toute information non brevetée sous support

[1371] Cass. 3e civ., 13 juill. 1966, pourvoi n°64-12,946, Bull.civ.III, n°358, p.316, JCP éd G 1967, II, n°15131, note Durand P.

[1372] Il s'agit de la possibilité de transmettre contractuellement le savoir-faire.

électronique relative à toute documentation, toute spécification ou tout procédé commercial, technique (fabrication, informatique …), marketing, financier et à tout projet de recherche de développement présent ou futur du Client. Le Client bénéficie d'un droit de propriété exclusif sur son savoir-faire et déclare n'accorder au Prestataire aucun droit sur son savoir-faire. Le Prestataire reconnaît que le Client est le propriétaire exclusif de son savoir-faire et qu'il ne dispose d'aucun droit sur le savoir-faire du Client. Le Prestataire s'engage à ne pas contrevenir à la confidentialité du savoir -faire et à ne pas accéder, traiter ou utiliser le savoir-faire hébergé dans l'infrastructure cloud sans le consentement préalable du Client. Afin de ne pas troubler la jouissance paisible du droit de propriété du Client sur son savoir-faire, le Prestataire s'interdit de réaliser une quelconque action ou manipulation technique, sur le savoir-faire du client, entendu largement et de manière non limitative comme : tout accès, toute utilisation, toute duplication, tout traitement, toute exploitation, toute représentation, toute reproduction, toute transmission.

En cas de contravention par le Prestataire à la présente disposition ainsi qu'aux droits intellectuel et de propriété du Client sur son savoir-faire, le Prestataire s'engage à réparer l'intégralité des préjudices qui résulteront de cette atteinte sans opposer une quelconque limitation de responsabilité dès lors que l'atteinte est avérée et lui est imputable.

En cas de contestation, les Parties peuvent décider, individuellement ou collectivement, de mandater un expert aux fins de constatations, de délimitation du champ de l'atteinte aux droits du Client sur son savoir-faire et de détermination de l'étendue du préjudice réparable. En cas de désaccord, les Parties s'engagent, en priorité, à privilégier la résolution du litige à l'amiable avant tout recours contentieux. ».

***588.*** Le savoir-faire est, ainsi, protégé par le secret spécifique du droit de la propriété intellectuelle et par l'intégration dans le contrat cloud d'une clause spécifique relative à la protection de ce savoir-faire. Il en résulterait qu'en cas d'atteinte à son savoir-faire par le prestataire de services, et en l'absence d'une résolution amiable du litige, le client, personne morale, pourra exercer une action en responsabilité contractuelle contre le prestataire de services cloud[1373], lorsque ce dernier aura manqué à son engagement de ne pas porter atteinte à la protection du savoir-faire. En outre, le Client, personne morale, conserve la faculté d'exercer une action en responsabilité civile délictuelle, et précisément, une action en concurrence déloyale[1374] contre le prestataire de services cloud en cas d'atteinte au savoir-faire.

[1373] V. *infra* n° 680 et suivants.

[1374] V. *infra* n° 635 et suivants.

***589.*** Après avoir envisagé la protection par le savoir-faire, il est envisagé d'étudier la protection par le secret de fabrique.

b) La protection par le secret de fabrique

***590.*** ***La protection légale du secret de fabrique***. À l'instar du savoir-faire, le client, personne morale, peut être amené, dans le cadre de l'exécution de son contrat de cloud computing, à héberger dans l'infrastructure en nuage les données relatives au secret de fabrique. Le secret de fabrique a été défini par la jurisprudence en 1935 comme étant « tout procédé de fabrication, offrant un intérêt pratique ou commerciale, mis en œuvre par un industriel et gardé secret à l'égard de ses concurrents »[1375]. Le secret de fabrique porte sur des procédés de fabrication et des caractéristiques techniques ayant pour objet la fabrication. En revanche, « si la jurisprudence exige généralement que ces moyens industriels aient une certaine originalité[1376], il n'est pas nécessaire qu'il s'agisse d'un procédé brevetable[1377]. Inversement, un moyen de fabrication qui sera brevetable, mais que son détenteur aura préféré garder secret plutôt que de le breveter sera également protégé par le secret de fabrique. En revanche, il est nécessaire que la technique soit gardée secrète : connue de tous, elle n'est plus protégeable »[1378]. De manière comparative par rapport au savoir-faire, il apparaît que les « connaissances couvertes par le secret de fabrique relèvent d'une catégorie plus vaste »[1379]. Il s'agit, alors, de données secrètes portant sur tous types de procédés de fabrication.

***591.*** ***La protection du secret de fabrique par le contrat cloud.*** À l'instar du savoir-faire, le secret de fabrique ne fait pas l'objet d'un droit privatif au profit de son détenteur (à la différence du brevet). Pour bénéficier de la protection par le secret de fabrique, il incombe au Client, personne morale, de préserver la confidentialité (le secret) de ces procédés de fabrication et des caractéristiques qui s'y rattachent. Dans le cadre d'un contrat de cloud computing, le Client, personne morale, qui envisage d'héberger des données relatives à son secret de fabrique dans le cloud, doit s'assurer que le contrat de cloud computing prévoit des dispositions protectrices concernant les données relatives à son secret de fabrique. À titre illustratif, en dépit que le secret de fabrique n'accorde aucun droit privatif à la personne morale, il est possible par convention

[1375] Cass. crim., 29 mars 1935, Bull. crim., p.350; V. également dans le même sens Cass. crim. 29 juin 1960, Bull. crim. p. 350.

[1376] Crim. 20 juin 1973, pourvoi n° 72-92.270, Ann. propr. ind. 1974. 85 ; également, V. Crim. 12 juin 1974, pourvoi n° 73-90.724, Ann. propr. ind. 1974. 97.

[1377] Crim. 16 mai 1862, Ann. propr. ind. 1862. p.221.

[1378] CA Paris, 13ème chambre, section B, 12 avr. 2002, Propr. ind. 2002, comm., n° 15, obs. Schmidt.

[1379] Azéma J., Galloux J-C, Précis Droit de la propriété industrielle, chap. 1 - La protection par le secret, Dalloz, coll. Précis, 8e éd., 2017

d'indiquer que cette dernière demeure propriétaire des données relatives à son secret de fabrique. En effet, le détenteur du secret n'a pas de droit de propriété (au sens juridique du terme) sur les informations non protégées par un titre de propriété intellectuelle ou industrielle (brevet, marque, droit d'auteur, dessins et modèles), mais le contrat peut indiquer une propriété au sens commun du terme désignant que le détenteur exerce, de manière exclusive, des prérogatives sur ses données couvertes par le secret.

***592.*** À l'instar de la protection conventionnelle du savoir-faire, il est possible de recourir à des clauses spécifiques telles que la clause relative à « l'obligation du Prestataire de non-accès, de non-traitement et de non-exploitation des données relatives au secret de fabrique du Client » ou bien d'indiquer cet engagement dans un acte annexé au contrat de cloud computing, tel qu'un accord de confidentialité. Il est proposé ci-après une proposition de rédaction de cette clause relative à « l'obligation du Prestataire de non-accès, de non-traitement et de non-exploitation des données relatives au secret de fabrique du Client » :

***593.*** « Dans le cadre des présentes, le Client n'accorde au profit du Prestataire aucune licence d'exploitation sur ses données, et en particulier, les données relatives au secret de fabrique (ci-après désignées « secret de fabrique ») hébergées dans l'infrastructure cloud du Prestataire. Il est entendu que les informations couvertes par le secret de fabrique sont protégées par les présentes et incluent de manière non limitative, toute information non brevetée sous support électronique, toute documentation, toute spécification d'un procédé de fabrication et/ou des caractéristiques techniques ayant pour objet la fabrication. Le Client bénéficie d'un droit de propriété exclusif sur son secret de fabrique et déclare n'accorder au Prestataire aucun droit sur les données couvertes par le secret de fabrique. Le Prestataire reconnaît que le Client est le propriétaire exclusif de son secret de fabrique et qu'il ne dispose d'aucun droit sur le secret de fabrique du Client. Le Prestataire s'engage à ne pas contrevenir à la confidentialité du secret de fabrique et à ne pas accéder, traiter ou utiliser le secret de fabrique hébergé dans l'infrastructure cloud sans le consentement préalable du Client. Afin de ne pas troubler la jouissance paisible du droit de propriété du Client sur son secret de fabrique, le Prestataire s'interdit de réaliser une quelconque action ou manipulation technique, sur le secret de fabrique, entendu largement et de manière non limitative comme : tout accès, toute utilisation, toute duplication, tout traitement, toute exploitation, toute représentation, toute reproduction, toute transmission.

En cas de contravention par le Prestataire à la présente disposition ainsi qu'aux droits intellectuels et de propriété du Client sur son secret de fabrique, le Prestataire s'engage à réparer l'intégralité des préjudices qui résulteront de cette atteinte sans opposer une quelconque limitation de responsabilité dès lors que l'atteinte est avérée et lui est imputable.

En cas de contestation, les Parties peuvent décider, individuellement ou collectivement, de mandater un expert aux fins de constatations, de délimitation du champ de l'atteinte aux droits du Client sur son secret de fabrique et de détermination de l'étendue du préjudice réparable. En cas de désaccord, les Parties s'engagent, en priorité, à privilégier la résolution du litige à l'amiable avant tout recours contentieux. ».

***594.*** À l'instar de la protection par le savoir-faire, le client, personne morale, titulaire d'un secret de fabrique pourra, en présence d'une atteinte au secret de fabrique et en l'absence d'une résolution amiable du litige, agir contre son prestataire de services cloud, dans le cadre d'une action en responsabilité contractuelle[1380] ou en concurrence déloyale[1381].

***595.*** Après l'étude du renforcement de la protection du patrimoine informationnel par le « secret » spécifique en droit de la propriété intellectuelle et industrielle, à savoir le savoir-faire et le secret de fabrique, il est procédé, à présent, à l'étude du renforcement de la protection du patrimoine informationnel par des droits spécifiques. `

## B) La protection du patrimoine informationnel par des droits spécifiques

***596.*** Au départ, le patrimoine informationnel a été utilisé par les personnes morales pour justifier l'exploitation de droits exclusifs sur les données afin d'enrichir et de protéger et valoriser le patrimoine informationnel. Ces données qui composant le patrimoine informationnel constituent, alors, pour la personne morale des actifs immatériels. Parmi ces droits exclusifs sur les données figurent le droit *sui generis* des producteurs sur la base de données et le droit d'auteur, qui sont, à présent, étudiés.

***597.*** ***Plan.*** Il est envisagé d'appréhender le droit *sui generis* des producteurs sur la base de données (1) et le droit d'auteur (2) afin de renforcer la protection du patrimoine informationnel de la personne morale dans le cadre de l'exécution d'un contrat de cloud computing.

### 1) L'application d'un droit sui generis du producteur de la base de données

***598.*** ***La protection des données par un droit privatif.*** Dans le contexte d'un renforcement de la protection du patrimoine informationnel de l'entreprise, l'exploitation de droits exclusifs a commencé à voir le jour depuis la consécration par la directive 96/9/CE du 11 mars 1996[1382] d'un

[1380] V. *infra* n° 681 et suivants.

[1381] V. *infra* n° 635 et suivants.

[1382] Dir. 96/9/CE du 11 mars 1996 concernant la protection juridique des bases de données.

droit *sui generis* sur les bases de données au bénéfice du producteur de la base de données. L'utilisation du « qualificatif latin « *sui generis* » semble *a priori* indiquer toute la singularité de ce droit »[1383]. La consécration de ce droit permet à la personne morale de jouir d'une « réservation des biens informationnels »[1384]. Cette directive a été transposée en France par la loi du 1er juillet 1998[1385]. En application de l'article 7 de la directive et l'article L. 342-1 du Code de la propriété intellectuelle, le producteur de la base de données peut interdire l'extraction et/ou la réutilisation de la totalité ou d'une partie, qualitativement ou quantitativement substantielle, du contenu de celle-ci, ainsi que l'extraction et/ou la réutilisation répétées et systématiques de parties non substantielles du contenu de la base de données qui supposeraient des actes contraires à une exploitation normale de cette base ou qui causeraient un préjudice injustifié aux intérêts légitimes du producteur[1386]. Ce droit sui generis a, ainsi, pour objet de sanctionner « des comportements fautifs (...) : un tiers tirant profit sans bourse délier d'une valeur économique protégée, en l'occurrence des investissements réalisés par le producteur »[1387]. En ce sens, ce droit sui generis se rapproche de la concurrence déloyale[1388] ou le parasitisme[1389] qui viennent également sanctionner des comportements fautifs. Bien que la directive européenne ait consacré ce droit sui generis afin de stimuler le stockage et le traitement de l'information[1390] et favoriser le marché des données[1391], il n'en demeure pas moins que l'appropriation de ces données par la personne morale permet de renforcer la protection de leurs données dans le cadre de l'exécution d'un contrat de cloud computing. En effet, le patrimoine informationnel renferme différents types de données de la personne morale et en particulier, une base de données. Concernant l'identification juridique d'une base de données, l'arrêté du 22 décembre 1981 l'a définie comme étant « un ensemble de données organisé en vue de son utilisation par des programmes correspondant à des applications distinctes et de manière à faciliter l'évolution indépendante des données »[1392]. Puis, les textes l'ont défini comme « un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou

---

[1383] Chatry S., La légitimité du droit sui generis du producteur de bases de données, Légipresse 2019 p.115.

[1384] Ibid.

[1385] L. nº 98-536, 1er juill. 1998, JO, 2 juill., nº 151, p. 10075.

[1386] Rambaud S., Droit sui generis des bases de données : vers un équilibre ? Revue Lamy Droit de l'Immatériel, Nº 49, 1er mai 2009.

[1387] Costes L., Perray R., Adda H. sous la direction de Costes L., Le Lamy droit du numérique (Guide), Partie 6 - Guide, Titre 5 Comment exploiter les bases de données et les créations multimédia ? Chapitre 3 Protection de l'ensemble informationnel, Section 2 Protection des bases de données, § 3. Protection par l'action en concurrence déloyale et en parasitisme, mis à jour 04/2022.

[1388] V. *infra* n° 635 et suivants.

[1389] V. *infra* n° 635 et 636.

[1390] Dir. 96/9/CE du 11 mars 1996 concernant la protection juridique des bases de données, consid. 12.

[1391] Rambaud S., Droit sui generis des bases de données : vers un équilibre ? Revue Lamy Droit de l'Immatériel, Nº 49, 1er mai 2009.

[1392] Arr. 22 déc. 1981, JONC 17 janv. 1982, p. 624 relatif à « l'enrichissement du vocabulaire de l'informatique ». V. également, Warusfel B., Mallet-Poujol N., Costes L. sous la direction de Vivant M., le Lamy droit du numérique, Partie 1 Numérique et biens, Division 2 Bases de données et autres ensembles informationnels, Chapitre 2 Protection des bases de données et autres ensembles informationnels, 205 - Des données aux ensembles de données, édition lamy expert, Wolterz Kluwer, mis à jour 04/2022.

méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen »[1393].

***599.*** S'agissant de la titularité du droit sui generis du producteur de la base de données, elle est accordée à la personne qui produit la base de données, appelée « producteur de bases de données »[1394]. Il s'agit d'une protection légale attachée uniquement au contenu de la base de données[1395] et non à l'architecture de cette base de données qui est considérée comme étant une œuvre d'esprit et est, donc, protégée par le droit d'auteur. [1396] Concernant le support, la base de données peut être sous forme papier ou sous forme numérique[1397]. Il en résulte que si l'architecture de la base de données est protégée par le droit d'auteur, le contenu de la base de données bénéficie d'une protection distincte et indépendante par ce « droit sui generis du producteur de la base de données[1398]. Par ce droit sui generis, ces données peuvent faire l'objet d'une appropriation privative au profit des personnes morales. Alors même que certains auteurs critiquent cette réservation exclusive des données, notamment lorsqu'elles concernent des données liées aux résultats de la recherche[1399], elle renforce considérablement le droit à la protection des données des personnes morales dans le cadre de l'exécution d'un contrat de cloud computing.

***600.*** ***Les conditions du droit sui generis du producteur de la base de données***. La CJCE a adopté une interprétation stricte des conditions de la protection[1400] et a maintenu une « une vision extensive de la notion d'« extraction »[1401] dans ses décisions[1402]. Cette interprétation est considérée par Madame Rambaud comme confirmant « la recherche d'un équilibre, entre une protection moins

---

[1393] Dir. 96/9/CE, art. 1, § 2 et art. L. 112-3, al. 2 CPI.

[1394] V. art. L341-1 CPI.

[1395] V. art. L341-1 CPI et v. art. 7.1 de la directive 96/9/CE.

[1396] V. art. L112-3 CPI. Le Conseil d'Etat a considéré que « la base de données est protégée par le droit d'auteur car elle ne constitue pas une simple collection de données mais un ensemble structuré et organisé d'informations » : Conseil d'Etat, Assemblée, du 10 juillet 1996 n° 168702 168734 169631 169951, publié au recueil Lebon. V. également, Civ 1ère, 22 septembre 2011 n° 10-23.073, inédit, la Cour de cassation a considéré que « M. Z. pouvait prétendre à la protection par le droit d'auteur pour l'architecture de la base de données ».

[1397] Considérant 14 de la directive 96/9/CE dispose qu' « il convient d'étendre la protection accordée par la présente directive aux bases de données non électroniques » et son article 1.1 ajoute que « la présente directive concerne la protection juridique des bases de données, quelles que soient leurs formes ». L'article 5 du traité de l'OMPI s'applique aux « compilations de données ou d'autres éléments, sous quelque forme que ce soit ». V. également, CA Paris, 4e ch., 12 septembre 2001, la cour d'appel de Paris a considéré qu'« il importe peu que cet ensemble d'informations soit communiqué au public sous forme d'un catalogue papier, l'existence d'une base de données ne dépendant pas de la nature de son support, lequel est différent ».

[1398] V. art. L341-1 CPI et v. art. 7.1 de la directive 96/9/CE.

[1399] Warusfel B., La protection des bases de données en question, un autre débat sur la propriété intellectuelle européenne, PI 2004. 896.

[1400] Rambaud S. et Lemarchand S., La CJCE précise les règles du jeu, Propr. intell. 2005, nº 14, p. 99 et s.

[1401] Rambaud S., Droit sui generis des bases de données : vers un équilibre ? Revue Lamy Droit de l'Immatériel, Nº 49, 1er mai 2009.

[1402] CJCE, 5 mars 2009, affaire C-545/07, Apis-Hristovich EOOD c/ Lakorda AD, RLDI 2009/48, nº 1571 ; Cass. 1re civ., 5 mars 2009, RLDI 2009/48, affaire nº 1572.

facilement accordée, mais une définition des actes pouvant être interdits relativement large »[1403]. Dans le cadre d'un contrat de cloud computing, le producteur de la base de données est le client, personne morale, qui utilise les services de cloud computing dans le cadre de son activité professionnelle. Pour que le client, personne morale, puisse bénéficier de cette protection, en sa qualité de producteur de la base de données, il doit satisfaire à des conditions matérielles et des conditions géographiques.

***601.*** S'agissant des conditions matérielles, l'article L 341-1 du CPI exige la réalisation d'un investissement financier, matériel ou humain qui doit être substantiel, qualitatif ou quantitatif pour la constitution, la vérification ou la présentation du contenu de la base de données[1404]. Le critère de *la réalisation d'un investissement financier, matériel ou humain* correspond à l'idée de déployer des moyens financiers ou d'emploi du temps d'efforts et d'énergie[1405]. Sur ce point, la jurisprudence est venue en préciser les contours de ce droit. Elle a reconnu la protection par le droit sui generis au producteur d'une base de données qui « justifie d'investissements tant en personnel qu'en prestations informatiques exclusivement consacrés auxdites bases en produisant à l'appui de leurs dires les contrats de travail et la facturation des prestations attestant que plusieurs personnes travaillent à temps complet à la constitution et à la vérification de celles-ci »[1406]. Elle a considéré, également, que la personne morale « ne s'est pas contentée de compiler ces données, mais « s'est investi » de façon substantielle pendant plusieurs années pour les réunir, les vérifier, les classer, les agencer en faisant des efforts de sélection et de conception » et qu'elle peut, donc bénéficier de la protection du droit sui generis du producteur de la base de données[1407]. Dans le sens contraire, les juges du fond ont estimé que « faute de justifier d'investissements financiers, matériels et humains substantiels dans la constitution, la vérification ou la présentation de sa base de données », la personne morale « ne peut bénéficier de la protection sui generis »[1408].

***602.*** Outre *la réalisation d'un investissement financier, matériel ou humain*, l'article L 341-1 du CPI exige, comme deuxième condition matérielle, que l'investissement soit substantiel, quantitatif et qualitatif[1409]. Le critère *substantiel* signifie que l'investissement soit suffisamment important par rapport au contenu obtenu[1410]. Sur ce point, les juges ont considéré que « l'appréciation du caractère substantiel doit […] s'opérer au regard non seulement des moyens

---

[1403] Rambaud S., Droit sui generis des bases de données : vers un équilibre ? Revue Lamy Droit de l'Immatériel, N° 49, 1er mai 2009.

[1404] V. également, CJUE, 9 novembre 2004, affaire n° C-203/02, The British Horseracing Board Ltd e.a. c/ William Hill Organization Ltd.

[1405] V. considérant 40 de la directive 96/9/CE.

[1406] CA Paris, 4e ch., section A, 12 septembre 2001, Tigest / Reed expositions France.

[1407] CA Bordeaux, 5e ch., 9 novembre 2006.

[1408] CA Paris, 2e ch., pôle 5, 23 mars 2012, RG n° 10/11168, Ryanair c/Opodo.

[1409] V. art. 7.1 de la directive 96/9/CE.

[1410] Ibid.

consacrés à l'obtention du contenu de la base de données, c'est-à-dire aux recherches, collecte et rassemblement des éléments nécessaires à la constitution de celle-ci (..) »[1411]. Il peut, également, s'agir d'un apport intellectuel chiffré par un expert [1412] d'un important investissement financier affecté à la production de la base de données[1413]. S'agissant du critère *quantitatif*, il correspond à l'idée de grandeur et de quantité et le critère *qualitatif* se rapporte à une notion subjective laissée à l'appréciation du juge[1414].

***603.*** Par ailleurs, l'article L341-1 du CPI exige, comme troisième condition matérielle, que l'investissement soit « pour la constitution, la vérification ou la présentation du contenu de la base de données »[1415]. Ce critère correspond à l'idée que l'investissement doit porter sur les moyens permettant de constituer le contenu de la base, le présenter et l'organiser[1416]. La jurisprudence est venue apporter des éléments de compréhension concernant la notion d'investissement. La CJUE a considéré que « la notion d'investissement lié à l'obtention du contenu d'une base de données […] doit s'entendre comme désignant les moyens consacrés à la recherche d'éléments existants et à leur rassemblement dans ladite base (...), les moyens en vue d'assurer la fiabilité de l'information contenue dans ladite base, au contrôle de l'exactitude des éléments recherchés, lors de la constitution de cette base ainsi que pendant la période de fonctionnement de celle-ci »[1417]. Les juges ont, ainsi, déterminé avec précision le périmètre de ce critère relatif à la notion d'investissement pour la constitution, la vérification ou la présentation du contenu de la base de données. Par ailleurs, les juges exercent un contrôle strict et refusent la protection par le droit sui generis lorsque « les investissements portent sur la création de données ou lorsque les investissements ne sont pas qualifiés »[1418].

***604.*** En sus des conditions matérielles, il est exigé des conditions géographiques. L'article L341-2 du code de la propriété intellectuelle précise qu'est admise au bénéfice de la protection par le droit sui generis, « les producteurs de bases de données, ressortissants d'un État membre de la Communauté européenne ou d'un État parti à l'accord sur l'Espace économique européen, ou qui ont dans un tel État leur résidence habituelle »[1419]. Il en résulte que la protection du droit sui generis des producteurs d'une base de données bénéficie uniquement aux personnes ressortissants d'un État

---

[1411] V. TGI Paris, 3e ch., 1ère section, 20 juin 2007, www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-3eme-chambre-1ere-section-jugement-du-20-juin-2007.

[1412] Com., 23 mars 2010, n° 08-20.427, 08-21.768, inédit, Lectiel / France Telecom.

[1413] CA Paris, 4e ch., section A, 18 février 2004.

[1414] V. art. 7.1 de la directive 96/9/CE.

[1415] V. art. 7.1 de la directive 96/9/CE et considérant 40 de la directive 96/9/CE.

[1416] CA Versailles, 14e ch., 17 février 2010.

[1417] CJUE, 9 novembre 2004, affaire C-203/02, v. également, CA Versailles, 14e ch., 17 février 2010.

[1418] Civ. 1re, 12 nov. 2015, n° 14-14.501.

[1419] V. art. L.341-2 du CPI qui transpose l'art. 11 de la directive 96/9/CE.

membre de la Communauté européenne ou d'un État parti à l'accord sur l'Espace économique européen, ou qui ont dans un tel État leur résidence habituelle.

***605.*** En définitive, pour que le client, personne morale, puisse bénéficier de la protection du droit sui generis des producteurs de la base de données, il doit remplir les conditions matérielles et géographiques. Si les conditions sont remplies, il pourra, en cas de violation de sa base de données par le prestataire de services, engager une action fondée sur l'atteinte au droit sui generis du producteur de la base de données.

***606.*** ***Une protection attachée à l'investissement.*** La protection dont bénéficie, le client, personne morale, en sa qualité de producteur de la base de données est attaché « à l'existence d'un investissement »[1420]. La titularité de ce droit est, ainsi, attribuée à l'investisseur « sans qu'aucune création ne fonde son existence »[1421], ce qui peut paraître atypique en droit de la propriété intellectuelle. En revanche, cette déconnexion avec la création a l'avantage d'accorder la titularité de ce droit à la personne morale qui s'est investie dans la production de la base de données et renforce par la même occasion la protection de son patrimoine informationnel.

***607.*** ***Des limitations non applicables dans le cadre d'un contrat de cloud computing.*** Le droit sui generis prévoit des limitations légales. En effet, ce droit ne permet pas de « s'opposer aux extractions ou réutilisations d'une partie non substantielle de la base de données »[1422]. Cette limitation n'est pas favorable au producteur de la base de données, puisqu'un tiers, désigné *utilisateur* « peut librement réutiliser les données extraites de manière non substantielle »[1423]. Également, ce droit sui generis ne permet pas de s'opposer à une extraction réalisée à des fins privées d'une partie substantielle du contenu d'une base de données non électronique[1424] ainsi qu'à des fins d'enseignement et de recherche[1425]. Dans le cadre d'un contrat de cloud computing conclu entre deux personnes morales de droit privé, il apparaît nécessaire de faire échec à ces limitations légales par l'intégration de clauses spécifiques. En effet, il ne faudrait pas que ces limitations puissent s'appliquer au profit du Prestataire de services cloud et au détriment du Client. Pour écarter ces limitations légales, le Client pourra invoquer l'obligation de loyauté attachée à tout contrat d'affaires et devra s'assurer que le contrat de cloud computing prévoit une interdiction au

[1420] Chatry S., La légitimité du droit sui generis du producteur de bases de données, Légipresse 2019 p.115.

[1421] Ibid.

[1422] Art. L. 342-1. CPI.

[1423] Chatry S., La légitimité du droit sui generis du producteur de bases de données, Légipresse 2019 p.115.

[1424] Art. L. 342-3, 2° CPI.

[1425] Art. L. 342-3, 4° CPI.

Prestataire d'accéder, d'exploiter et de traiter ses données[1426]. Il est, donc, suggéré d'intégrer dans le champ contractuel, le droit sui generis du client et d'écarter expressément par convention ces limitations légales afin de renforcer la protection de la base de données héberger dans le cloud.

***608. La retranscription conventionnelle du droit sui generis dans le contrat de cloud computing***. Pour un souci de renforcement du patrimoine informationnel de la personne morale dans le cloud computing, il est suggéré d'insérer dans le contrat de cloud computing une clause intitulée "Obligation du Prestataire de non-extraction et/ou de non-réutilisation du contenu de la base de données du Client". Il est proposé ci-après une proposition de rédaction de cette clause :

« Dans le cadre des présentes, le Client n'accorde au profit du Prestataire aucune licence d'exploitation du contenu de ses bases de données hébergées dans l'infrastructure cloud du Prestataire. La base de données est entendue, ici, largement et de manière non limitative comme étant « un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen » (Art. L112-3 CPI). Le Client bénéficie d'un droit de propriété exclusif sur ses bases de données et déclare n'accorder au Prestataire aucun droit sur ses bases de données. Le Prestataire reconnaît que le Client est le propriétaire exclusif de ses bases de données hébergées dans l'infrastructure cloud et qu'il ne dispose d'aucun droit sur les bases de données du Client. Le Prestataire s'engage à ne pas accéder, traiter, utiliser et exploiter les bases de données hébergées dans l'infrastructure cloud sans le consentement préalable du Client. Afin de ne pas troubler la jouissance paisible du droit de propriété de son Client sur ses bases de données, le Prestataire s'interdit de réaliser une quelconque action ou manipulation technique, sur les bases de données de son Client, entendu largement et de façon non limitative comme : tout traitement, toute exploitation, toute représentation, toute reproduction, toute extraction et/ou réutilisation totale ou partielle d'une partie substantielle ou non de la base de données.

En cas de contravention par le Prestataire à la présente disposition ainsi qu'aux droits intellectuels et au droit de propriété du Client sur ses bases de données, le Prestataire s'engage à réparer l'intégralité des préjudices qui résulteront de cette atteinte sans opposer une quelconque limitation de responsabilité dès lors que l'atteinte est avérée et lui est imputable.

En cas de contestation, les Parties peuvent décider, individuellement ou collectivement, de mandater un expert aux fins de constatations, de délimitation du champ de l'atteinte aux droits du Client sur ses bases de données et de déterminer l'étendue du préjudice réparable. En cas de

[1426] Archambault L., Migeon N., Traitement de données et cloud, Gaz. Pal. 31 août 2021, n° 425 s1, p. 14.

désaccord, les Parties s'engagent, en priorité, à privilégier la résolution du litige à l'amiable avant tout recours contentieux. »

***609.*** En application de l'obligation de loyauté et des prescriptions prévues dans la clause de non-exploitation de la base de données, le prestataire de services engage sa responsabilité délictuelle[1427] ou contractuelle[1428], en cas d'atteinte au droit sui generis à la base de données du client.

***610.*** ***Une évolution législative attendue.*** Malgré une définition qui intègre les bases de données électroniques et non électroniques[1429], celle-ci est dépassée par les progrès technologiques. Ce droit sui generis ne semblerait pas pouvoir s'appliquer à l'ensemble des données, en particulier les données qui seraient produites « par des machines, dispositifs de l'Internet des objets, mégadonnées, intelligence artificielle, etc. »[1430]. Cette exclusion est critiquable dans la mesure, comme l'affirme Monsieur Chatry « les investissements pourtant colossaux portent davantage sur la génération de données puis l'interconnexion des données et non pas sur l'obtention, la constitution ou la présentation de ces données »[1431]. Il résulte que si le droit sui generis renforce la protection des données de la personne morale dans le cadre d'un cloud computing, il est attendu que ce droit élargisse son champ d'application à l'ensemble des données pour renforcer davantage la protection des données des personnes morales dans les contrats de cloud computing. En attendant, il est possible de renforcer le droit sui generis du Client en aménageant les dispositions du contrat de cloud computing.

***611.*** En définitive, le droit sui generis du producteur de la base de données permet de concourir avec les droits identifiés dans cette étude au renforcement de la protection des données des personnes morales. Après avoir étudié le droit sui generis, il est question, à présent, d'envisager l'application du droit d'auteur au renforcement de la protection du patrimoine informationnel de la personne morale dans les contrats de cloud computing.

---

[1427] Il est possible d'agir sur le fondement du droit sui generis du producteur de la base de données ainsi que sur le fondement de la concurrence déloyale : v. *infra* n° 634 et suivants (resp. délictuelle).

[1428] V. *infra* n° 682 et suivants (resp. contractuelle).

[1429] V. *supra* n° 594.

[1430] Evaluation of Directive 96/9/EC on the legal protection of databases, SWD (2018) 147 final, p. 15 et 24, dans Chatry S., La légitimité du droit sui generis du producteur de bases de données, Légipresse 2019.

[1431] Chatry S., La légitimité du droit sui generis du producteur de bases de données, Légipresse 2019 p.115.

**2) L'application des droits d'auteur**

***612. La protection des œuvres par le droit d'auteur.*** Dans le cadre d'un contrat de cloud computing, les personnes morales peuvent être amenées à héberger dans le cloud des œuvres dématérialisées. Pour la doctrine, « la protection des œuvres dématérialisées constitue, en effet, un impératif à la fois pour les auteurs et pour les acteurs du monde économique »[1432]. La question de la protection légale des œuvres dématérialisées des personnes morales se pose en particulier lorsqu'elles concluent un contrat de cloud computing. En droit français, c'est le droit d'auteur qui protège les œuvres de l'esprit des personnes morales[1433]. En effet, ce droit est considéré comme étant le droit des créateurs. Le droit d'auteur est consacré à l'article L.111-1 du code de la propriété intellectuelle. Cet article dispose que « l'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous. Ce droit comporte des attributs d'ordre intellectuel et moral ainsi que des attributs d'ordre patrimonial. Pour bénéficier de cette protection, la donnée doit présenter un caractère original[1434], c'est-à-dire l'œuvre doit être marquée de l'empreinte de la personnalité de l'auteur. Le bénéficie de la protection du droit d'auteur est conférée, ainsi, à l'auteur du seul fait de la création d'une œuvre originale. Le titulaire du droit d'auteur pourra alors faire interdire tout acte de reproduction ou de représentation de l'information réalisé en violation de ce droit.

***613. Le contenu du droit d'auteur***. Les prérogatives relevant du droit moral n'appartiennent qu'à la personne de l'auteur et ne sont pas cessibles (paternité, respect, divulgation, retrait et repentir)[1435]. S'agissant des attributs d'ordre patrimonial[1436], l'auteur dispose d'un droit d'exploitation, lequel qui comprend un droit de représentation et un droit de reproduction[1437]. Le droit de représentation est défini comme étant « le droit pour l'auteur d'autoriser ou d'interdire la représentation de son œuvre »[1438] et la représentation consiste en « la communication de l'œuvre au public par un procédé quelconque »[1439]. Le droit de reproduction vise toute exploitation qui suppose une fixation de

[1432] Bitan H., Droit et expertise du numérique, Créations immatérielles, Données personnelles, E.réputation, Droit à l'oubli, Neutralité, Responsabilité civile et pénale, édition Lamy, collection Axe droit, Wolters Kluwer, juin 2015.

[1433] Caron C., Droit d'auteur et droits voisins, édition LexisNexis, coll. Manuels, 6e éd., septembre 2020.

[1434] Warusfel B., Mallet-Poujol N., Costes L. sous la direction de Vivant M., le Lamy droit du numérique, Partie 1 Numérique et biens, Division 2 Bases de données et autres ensembles informationnels, Chapitre 2 Protection des bases de données et autres ensembles informationnels, 205 - Des données aux ensembles de données, édition lamy expert, Wolterz Kluwer, mis à jour 04/2022.

[1435] Protection du patrimoine informationnel, CIGREF, - FedISA, 2007.

[1436] Article L 122-1 et suivants du code de la propriété intellectuelle (CPI)

[1437] V. art. L.122-1 du CPI.

[1438] Dormont S., Droits patrimoniaux, Répertoire IP/IT et Communication, droit d'auteur, septembre 2019.

[1439] V. art. L.122-2 du CPI.

l'œuvre destinée au public »[1440] et la reproduction consiste en « la fixation matérielle de l'œuvre par tous les procédés qui permettent de la communiquer au public d'une manière indirecte »[1441]. La reproduction concerne toute reproduction d'œuvre sur un support quelconque, matériel ou immatériel afin d'être communiquée au public[1442]. En conséquence, sont visées les reproductions immatérielles, lesquelles peuvent être hébergées dans une infrastructure cloud.

***614.*** En outre, l'article L 122-1 du CPI énumère les attributs patrimoniaux du droit de propriété de l'auteur sur ses œuvres. Cette énumération est critiquée par la doctrine qui considère que la mention du terme « comprend » pour décrire le droit d'exploitation permet de conclure que l'énumération des droits identifiés (un droit de représentation et un droit de reproduction) n'est pas limitative[1443]. La doctrine estime que « le droit d'exploitation qui appartient à l'auteur comprend en réalité, en plus : du droit de représentation et de reproduction, les droits suivants : le droit de communication au public, ou le droit de mise à disposition du public ; le droit de distribution ou le droit de mise en circulation ; le droit de destination ; le droit de traduction ; le droit d'adaptation, d'arrangement et d'autres transformations ; le droit de synchronisation en matière musicale ; le droit de location ; le droit de prêt ; le droit d'exposition pour les œuvres plastiques et graphiques ; le droit de suite en matière d'œuvres graphiques et plastiques »[1444]. En sus du droit de représentation et de reproduction qui composent le droit d'exploitation, la personne morale dispose d'un droit de suite qui « permet à l'auteur d'une œuvre de suivre pécuniairement le destin du support matériel de son œuvre »[1445]. Ce droit de suite ne constitue pas « une faculté pour l'auteur de s'opposer ou d'autoriser la vente de l'œuvre : il s'agit purement d'un droit à rémunération d'un type particulier, non d'un droit exclusif »[1446]. Également, la personne morale dispose d'un droit de distribution qui correspond au droit d'autoriser ou interdire la vente (l'original de l'œuvre) ou au moins l'aliénation d'exemplaires matériels de l'œuvre (copies de l'œuvre) au public[1447]. Ce droit concerne, également, le support matériel de l'œuvre or notre étude s'intéresse aux œuvres hébergées dans le cloud, donc aux œuvres immatérielles. En outre, la personne morale dispose d'un droit de location qui correspond au droit exclusif « pour l'auteur d'autoriser ou d'interdire la location d'exemplaires matériels de ses œuvres ». La location est définie par la directive n° 2006/113/CE comme « la mise à disposition pour l'usage, pour un temps limité et pour un avantage

[1440] Dormont S., Droits patrimoniaux, Répertoire IP/IT et Communication, droit d'auteur, septembre 2019.

[1441] V. art. L.122-3 du CPI.

[1442] Dormont S., Droits patrimoniaux, Répertoire IP/IT et Communication, droit d'auteur, septembre 2019.

[1443] Bertrand R. A., Droits de l'auteur, chap. 106, Dalloz action Droit d'auteur, 2010.

[1444] Ibid.

[1445] Dormont S., Droits patrimoniaux, Répertoire IP/IT et Communication, droit d'auteur, septembre 2019.

[1446] Ibid.

[1447] Ibid.

économique ou commercial direct ou indirect »[1448] d'exemplaires de l'œuvre »[1449]. À l'instar des autres droits étudiés ci-dessus, ce droit de contrôler la location de l'œuvre porte uniquement sur un support matériel et n'intéresse, donc, pas notre étude laquelle porte sur les données hébergées dans l'infrastructure cloud. Enfin, l'auteur, également, dispose d'un droit de prêt qui est défini comme un droit exclusif « pour l'auteur d'autoriser ou d'interdire le prêt d'exemplaires matériels de ses œuvres » [1450]. Il s'agit, ainsi, d'une mise à disposition de l'œuvre sur un support matériel pour un usage et une durée limitée. Ce droit, également, concerne uniquement les œuvres sur un support matériel et non immatériel. Après avoir identifié le contenu du droit d'auteur, il est envisagé d'étudier le bénéfice du droit d'auteur à une personne morale pour protéger certaines données de son patrimoine informationnel.

***615. Le contournement de la difficulté juridique de la titularité du droit d'auteur au profit de la personne morale.*** Le droit d'auteur pose une difficulté juridique au regard de la titularité de ce droit qui est réservée, d'après une analyse des textes[1451], à la personne physique. Le principe du droit d'auteur est posé à l'article L.111-1 du CPI : « L'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous. Ce droit comporte des attributs d'ordre intellectuel et moral, ainsi que des attributs d'ordre patrimonial... ». Cet article fait référence à la création, notion qui nous permet d'en déduire que l'activité créatrice ne peut que provenir d'un créateur, personne physique et non d'une personne morale. Ce postulat a pour source une philosophie humaniste du droit d'auteur qui a pour « principe que seule la personne physique peut prétendre à la qualité d'auteur, puisqu'elle seule peut être douée de sensibilité et d'esprit créatif »[1452]. Cette théorie qualifiée de « personnaliste » procède « du courant qui voit dans la personne morale une fiction, une entité qui ne comporte ni corps ni âme (en dehors de ses membres) ne pouvant faire activité créatrice »[1453]. De même, la référence aux attributs de l'auteur, dans l'article susvisé, se rattache, également, en application de l'article L. 121-1 et suivants du CPI[1454], à l'auteur, personne physique. La doctrine a considéré que cette référence à la

[1448] Directive 2006/113/ce du parlement européen et du conseil du 12 décembre 2006 relative à la qualité requise des eaux conchylicoles.

[1449] Dormont S., Droits patrimoniaux, Répertoire IP/IT et Communication, droit d'auteur, septembre 2019.

[1450] Dormont S., Droits patrimoniaux, Répertoire IP/IT et Communication, droit d'auteur, septembre 2019.

[1451] V. art. L. 111-1 du CPI et art. L.121-1 et suivants CPI.

[1452] Cervetti D., La personne morale (encore) évincée de la qualité d'auteur, RLDI n° 114, 1er avril 2015.

[1453] Vivant M., Bruguière J-M, Les titulaires du droit d'auteur, Titre 2 - Les titulaires du droit d'auteur, Chapitre 1 - Les principes directeurs, Droit d'auteur et droits voisins, Précis, Dalloz, 4e édition, 01/2019.

[1454] Art. L.121-1, CPI : « L'auteur jouit du droit au respect de son nom, de sa qualité et de son œuvre. Ce droit est attaché à sa personne. Il est perpétuel, inaliénable et imprescriptible. Il est transmissible à cause de mort aux héritiers de l'auteur. L'exercice peut en être conféré à un tiers en vertu de dispositions testamentaires ».

création et aux attributs patrimoniaux « est perçue comme antinomique de l'état des personnes »[1455]. En matière de cloud computing, cette éviction a pour effet de contrarier les droits d'agirde la personne morale pour la défense de certaines données de son patrimoine intellectuel à l'égard de son Prestataire de services cloud. Sur ce point, la Cour de cassation est venue, également, lever toute ambiguïté concernant la titularité du droit d'auteur, en considérant qu'« une personne morale ne peut avoir la qualité d'auteur »[1456]. Cette décision affirme sans équivoque l'éviction des personnes morales de la qualité d'auteur et réaffirme, ainsi, la conception personnaliste du droit d'auteur. Cette jurisprudence a été considérée par la doctrine comme posant « en véritable dogme que l'auteur dont le droit assure la protection est forcément le créateur de l'œuvre »[1457]. L'ensemble de la doctrine s'accorde pour reconnaître que plusieurs systèmes peuvent coexister pour déterminer l'auteur[1458]. En revanche, cette éviction des personnes morales de la qualité d'auteur qui s'appuie sur une conception personnaliste du droit d'auteur est remise en cause par une partie de la doctrine. Les opposants à cette conception personnaliste du droit d'auteur fondent leur théorie sur une conception plus pragmatique du droit d'auteur laquelle est fondée sur approche économique permettant de conférer, ainsi, « la qualité d'auteur à la personne morale qui a participé à la réalisation de l'œuvre, à quelque degré que ce soit »[1459]. Pour conforter cette conception fondée sur une approche économique, il est mis en avant dans l'étude de Monsieur Cervetti, la nécessité, dans un contexte de mondialisation des échanges économiques et de circulation de l'information, de se rapprocher avec les pays de copyrigh qui admettent la qualité d'auteur aux personnes morales[1460]. Il est cité l'exemple du « Copyright Act américain de 1976 », qui reconnaît l'employeur comme étant l'auteur et possède tous les droits compris dans le copyright. Il est, également, préconisé de prendre en considération le degré de participation de la personne morale dans la réalisation de son œuvre immatérielle composant son patrimoine informationnel. Dans certaines décisions, il apparaît que le juge décide de prendre de la distance avec cette vision personnaliste du droit d'auteur en acceptant de « tenir une personne morale pour auteur ou au moins de lui reconnaître les traits d'un auteur »[1461]. À titre illustratif, la première chambre civile de la Cour de cassation, dans un arrêt du 24 mars 1993, a considéré que « l'exploitation économique de l'œuvre fait présumer la titularité des

[1455] Warusfel B., Mallet-Poujol N., Costes L. sous la direction de Vivant M., le Lamy droit du numérique, Partie 1 Numérique et biens, Division 2 Bases de données et autres ensembles informationnels, Chapitre 2 Protection des bases de données et autres ensembles informationnels, 205 - Des données aux ensembles de données, édition lamy expert, Wolterz Kluwer, mis à jour 04/2022.

[1456] Cass. 1re civ., 15 janv. 2015, pourvoi 13-23.566, bull.2015, I, n° 11.

[1457] Cervetti D., La personne morale (encore) évincée de la qualité d'auteur, RLDI n° 114, 1er avril 2015.

[1458] Ibid.

[1459] Ibid.

[1460] Ibid.

[1461] Vivant M., Bruguière J-M, Les titulaires du droit d'auteur, Titre 2 - Les titulaires du droit d'auteur, Chapitre 1 - Les principes directeurs, Droit d'auteur et droits voisins, Précis, Dalloz, 4e édition, 01/2019.

droits de la personnalité morale »[1462]. Concernant cette évolution jurisprudentielle, le professeur Vivant a estimé que « si la jurisprudence perçoit la nécessité de donner aux personnes morales une place que la loi ne leur reconnaissait pas, c'est certainement en considération de ce qu'est présentement devenue la création. Le fait est que la notion d'auteur sur la base de laquelle s'est édifié notre système ne correspond plus guère aux conditions dans lesquelles naissent aujourd'hui les œuvres »[1463]. À travers cette évolution jurisprudentielle, il s'agit de passer d'une approche fondée sur une vision personnaliste du droit d'auteur à une vision économique, laquelle serait plus pragmatique et conforme à la réalité actuelle du contexte de création des œuvres.

***616.*** De cette analyse, se pose la question de savoir s'il ne serait pas légitime de conférer la qualité d'auteur à la personne morale lorsqu'elle s'est investie activement dans la réalisation de l'œuvre par la mise à disposition de ressources financières et humaines. En attendant une évolution du droit d'auteur français et européen, il est suggéré d'envisager avec plus de souplesse la détermination du titulaire des droits lorsque l'œuvre est initiée par une personne morale. Pour échapper à l'éviction des personnes morales de la qualité d'auteur, il est proposé de recourir à la notion d'œuvre collective[1464]. Il est, donc, envisagé d'étudier la notion d'œuvre collective afin de permettre au client, personne morale, dans le cadre d'un contrat de cloud computing de bénéficier de la protection dévolue à l'auteur.

***617. Le renforcement de la protection par les droits d'auteur de la personne morale sur l'œuvre collective***. L'œuvre « est dite collective l'œuvre créée sur l'initiative d'une personne physique ou morale qui l'édite, la publie et la divulgue sous sa direction et son nom et dans laquelle la contribution personnelle des divers auteurs participant à son élaboration se fond dans l'ensemble en vue duquel elle est conçue, sans qu'il soit possible d'attribuer à chacun d'eux un droit distinct sur l'ensemble réalisé »[1465]. Concrètement, il s'agit d'identifier une personne physique ou morale qui prend l'initiative de la réalisation de l'œuvre ; dirige cette réalisation et la livre au public. Si ce texte permet de conférer au profit de la personne morale le bénéfice des droits d'auteurs, la particularité, ici, est que ces droits s'exercent en concours avec les autres droits d'auteurs des personnes physiques sur cette œuvre. L'œuvre collective est, ici, issue d'une contribution collective. Il en résulte que « chacun peut voir sa contribution identifiée, ou non, mais aucun ne

[1462] Civ. 1re, 24 mars 1993, JCP 1993. II. 22085, note F. Greffe ; RTD com. 1995. 418, obs. Françon.

[1463] Vivant M., Bruguière J-M, Les titulaires du droit d'auteur, Titre 2 - Les titulaires du droit d'auteur, Chapitre 1 - Les principes directeurs, Droit d'auteur et droits voisins, Précis, Dalloz, 4e édition, 01/2019.

[1464] Warusfel B., Mallet-Poujol N., Costes L. sous la direction de Vivant M., le Lamy droit du numérique, Partie 1 Numérique et biens, Division 2 Bases de données et autres ensembles informationnels, Chapitre 2 Protection des bases de données et autres ensembles informationnels, 205 - Des données aux ensembles de données, édition lamy expert, Wolterz Kluwer, mis à jour 04/2022.

[1465] Art. L. 113-2, al. 3, CPI.

peut, par sa contribution, se voir reconnaître un droit sur le tout »[1466]. L'un des auteurs sur l'œuvre collective est auteur de sa contribution, mais ne peut prétendre « avoir un droit sur le tout »[1467], c'est-à-dire sur l'œuvre dans son ensemble. Afin d'échapper à cette contrainte reposant sur une division des droits d'auteur sur l'œuvre collective, et ainsi renforcer la protection du patrimoine informationnel de la personne morale dans le contrat de cloud computing, il est proposé de reprendre l'analyse pragmatique du professeur Th. Revet. Lorsque l'œuvre collective est créée au profit d'une personne morale de droit privé par ses salariés, il considère que cette réalisation a pour cadre juridique le contrat de travail et que, « juridiquement, les produits d'un travail salarié ont donc pour auteur l'employeur et non le salarié : ce résultat est la conséquence mécanique de la maîtrise de la force de travail dès avant et tout au long de sa mise en œuvre »[1468]. Cette analyse a, ainsi, pour effet d'admettre que dans une création d'œuvre réalisée par des employées d'une société, personne morale de droit privé, la titularité du droit d'auteur sera dévolue uniquement et entièrement à cette dernière. Il s'agirait ainsi d'admettre, selon la doctrine, que la personne morale de droit privé en tant qu'instigatrice de l'œuvre va rassembler « les contributions individuelles en une entité unique les absorbent afin que la conception de l'ensemble échappe aux contributeurs ; ces derniers ne pouvant plus prétendre à un droit indivis sur le tout »[1469]. En l'espèce, il s'agirait, ainsi, d'admettre une théorie de la réalité au profit de la reconnaissance des droits d'auteur à la personne morale[1470]. Il est rappelé par la doctrine que « des personnes morales organisent le processus de création, distribuent leur produit, ont un intérêt à protéger leur création. En d'autres termes, risquons ce propos hérétique : des personnes morales créent »[1471]. Il apparaît que cette réalité économique s'est imposée au juge[1472]. Il en résulte de cette analyse que si la création intellectuelle est qualifiée d'œuvre collective, alors dans ce cas la personne morale sera investie de ces droits d'auteur, y compris des attributs moraux[1473].

---

[1466] Warusfel B., Mallet-Poujol N., Costes L. sous la direction de Vivant M., le Lamy droit du numérique, Partie 1 Numérique et biens, Division 2 Bases de données et autres ensembles informationnels, Chapitre 2 Protection des bases de données et autres ensembles informationnels, 205 - Des données aux ensembles de données, édition lamy expert, Wolterz Kluwer, mis à jour 04/2022.

[1467] Ibid.

[1468] Revet Th., La qualité d'auteur d'une œuvre de l'esprit, obs. sous Cass. 1re civ., 22 mars 2011, nº 11-10.132. Du même auteur, La force de travail, préf. F. Zenati, Litec, 1992, nº 240 et, s'agissant de l'œuvre collective, n° 243 et 511.

[1469] Cervetti D., La personne morale (encore) évincée de la qualité d'auteur, RLDI n° 114, 1er avril 2015.V. également, Vivant M. et Bruguière J.-M., Droit d'auteur et droits voisins, Dalloz, 4e éd., 2019. V. également, au soutien de la thèse qu'une personne morale peut développer une personnalité artistique propre : Fouilland F., L'auteur personne morale, éléments pour une théorie de l'emprunt de personnalité artistique, Comm. com. électr. 2008, nº 12, étude 24.

[1470] V. les positions de Jean-Michel Bruguière qui défend l'idée selon laquelle les droits de la personnalité doivent être reconnus (avec certaines inflexions) aux personnes morales ; voir notamment J.-M. Bruguière et B. Gleize, Droits de la personnalité, Ellipses, 2015, p. 48 s.

[1471] Vivant M., Bruguière J-M, Les titulaires du droit d'auteur, Titre 2 - Les titulaires du droit d'auteur, Chapitre 1 - Les principes directeurs, Droit d'auteur et droits voisins, Précis, Dalloz, 4e édition, 01/2019.

[1472] V. *supra* n°608.

[1473] Cervetti D., La personne morale (encore) évincée de la qualité d'auteur, RLDI n° 114, 1er avril 2015.V. également, Vivant M. et Bruguière J.-M., Droit d'auteur et droits voisins, Dalloz, 4e éd., 2019.

***618.*** Il est question à présent d'appréhender comment ces droits d'auteurs vont pouvoir être intégrés dans le contrat de cloud computing afin de renforcer la protection des œuvres dématérialisées de la personne morale.

***619. La retranscription conventionnelle des droits d'auteur dans le contrat de cloud computing***. S'agissant les attributs d'ordre patrimonial et en particulier le droit d'exploitation, il apparaît qu'en matière de cloud computing, le prestataire de services cloud n'est pas autorisé à exploiter à son profit les œuvres dématérialisées de son client, personne morale sans le consentement de ce dernier. Pour renforcer la protection du patrimoine informationnel numérique de la personne morale, il est proposé d'insérer dans le contrat cloud une clause intitulée "obligation du Prestataire de non-exploitation des œuvres du Client" laquelle intégrera l'interdiction de la représentation et de la reproduction de l'œuvre. Il est proposé, ci-après, une proposition de rédaction de cette clause :

« Dans le cadre des présentes, le Client n'accorde au profit du Prestataire aucune licence d'exploitation sur ses œuvres de l'esprit lesquelles sont hébergées dans l'infrastructure cloud du Prestataire. Les œuvres de l'esprit sont entendues, ici, largement et de manière non limitative comme étant celles mentionnées à l'article L.112-2 du code de la propriété intellectuelle. Le Client bénéficie d'un droit de propriété exclusif sur ses œuvres et dispose des attributs d'ordre moral (paternité, respect, divulgation, retrait et repentir concernant l'œuvre) et patrimonial (droit d'exploitation comprenant un droit de reproduction et de représentation). Le Client déclare n'accorder au Prestataire aucun droit sur ses œuvres de l'esprit. Le Prestataire reconnaît que le Client est le propriétaire exclusif de ses œuvres et qu'il ne dispose d'aucun droit sur les œuvres de son Client. Le Prestataire s'engage à ne pas utiliser, traiter, exploiter les œuvres de l'esprit hébergées dans l'infrastructure cloud sans le consentement préalable du Client. Afin de ne pas troubler la jouissance paisible du droit de propriété du Client sur ses œuvres, le Prestataire s'interdit de réaliser une quelconque action ou manipulation technique, sur les œuvres du Client, entendu largement et de manière non limitative comme : toute utilisation, toute duplication, tout traitement, toute exploitation, toute représentation, toute reproduction et toute transmission.

En cas de contravention par le Prestataire à la présente disposition ainsi qu'aux droits intellectuels et au droit de propriété du Client sur ses œuvres, le Prestataire s'engage à réparer l'intégralité des préjudices qui résulteront de cette atteinte sans opposer une quelconque limitation de responsabilité dès lors que l'atteinte est avérée et lui est imputable.

En cas de contestation, les Parties peuvent décider, individuellement ou collectivement, de mandater un expert aux fins de constatations, de délimitation du champ de l'atteinte aux droits du

Client sur ses œuvres et de déterminer l'étendue du préjudice réparable. En cas de désaccord, les Parties s'engagent, en priorité, à privilégier la résolution du litige à l'amiable avant tout recours contentieux. ».

***620.*** Si certaines données du patrimoine informationnel de la personne morale hébergées dans le cloud peuvent être protégées par le droit sui generis du producteur de la base de données et par le droit d'auteur, il demeure que plusieurs données ne vont pas être couvertes par ces droits spécifiques ; se pose, donc, pour celles-ci la question de leur protection juridique. La résolution de cette question est appréhendée, dans la partie suivante, à travers l'intervention du droit commun des affaires.

## Section 2 : Le renforcement de la protection des données par le droit de commun des affaires

***621.*** Après avoir étudié le renforcement de la protection des données de la personne morale dans les contrats de cloud computing par l'application du droit de la propriété intellectuelle et industrielle, il est proposé, à présent, d'étudier le renforcement de la protection des données par le droit de commun des affaires. Selon F. Hagel, l'entreprise se doit de protéger les informations en sa possession et précise que si « le brevet ne peut protéger que des inventions, le secret est applicable, si on se limite à la sphère de la technologie, à tout type d'information technique et commerciale ayant une valeur du fait qu'elle n'est pas accessible aux tiers – ce qui va bien au-delà des tours de main et secrets de fabrication correspondant à l'acception traditionnelle du terme « savoir-faire ». Une des solutions, ainsi, envisagées au renforcement de la protection des données de la personne morale, est le « secret » et particulièrement le secret des affaires. En effet, c'est dans un objectif de renforcement de la protection des données confidentielles des personnes morales, que le législateur a consacré au profit des personnes morales, le droit au « secret des affaires » lequel a permis, également, d'élargir les voies d'actions existantes en matière de responsabilité délictuelle.

***622.*** ***Plan.*** Il est envisagé d'étudier, le renforcement de la protection du patrimoine informationnel par le secret des affaires (A) et par un élargissement des actions en responsabilité délictuelle (B).

## A) Le renforcement de la protection du patrimoine informationnel par le secret des affaires

***623.*** Tel qu'affirmé par Monsieur Saint-Aubin à propos des nouveaux enjeux juridiques des données, que « le droit s'adapte progressivement aux nouvelles exigences de l'intelligence économique et tend à consacrer des droits réservés aux entreprises sur leurs données »[1474]. Avant, la protection du « secret » était réservée, par le droit de la propriété intellectuelle et industrielle, à certains types de données qui contenaient soit un savoir-faire, soit un secret de fabrique. Cette fois, avec le « secret des affaires », la protection est élargie à l'ensemble des données confidentielles de la personne morale.

***624.*** ***Plan.*** La consécration du secret des affaires permet de renforcer la protection du patrimoine informationnel grâce à un élargissement du champ de la protection (1) et par l'établissement de mesures spécifiques (2).

### 1) L'élargissement du champ de la protection des données par le secret des affaires

***625.*** ***La consécration légale du secret des affaires***. L'Union européenne « prenant conscience que le secret constitue une voie essentielle pour l'appropriation des innovations des entreprises (…) a souhaité harmoniser l'appréhension légale de ces secrets pour faciliter le fonctionnement du marché intérieur »[1475]. Ce travail d'harmonisation s'est concrétisé par l'adoption de la Directive du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulguées (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites[1476]. En effet, il est mis en avant la nécessité de protéger le patrimoine informationnel de l'entreprise en ce qu'il a une forte valeur financière au titre de l'actif immatériel de l'entreprise[1477]. La solution proposée est, ainsi, le secret des affaires. La consécration du « secret des affaires » permet d'avoir une catégorie générique de données lesquelles ont pour caractéristique principale d'être secrètes. Il s'agit, très clairement, d'un élargissement du champ des données pouvant prétendre à la protection par le secret et non uniquement les données qui renferment un savoir-faire ou un secret de fabrique.

---

[1474] Saint-Aubin Th., les nouveaux enjeux juridiques des données (big data, web sémantique et linked data ) Les droits de l'opérateur de données sur son patrimoine numérique informationnel, Revue Lamy Droit de l'Immatériel, N° 102, 1er mars 2014.

[1475] Binctin N., Répertoire IP/IT et Communication- Savoir-faire, Janvier 2018.

[1476] Directive européenne n° 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulguées (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, publiée au JOUE le 15 juin 2016.

[1477] Livre blanc du CIGREF -FedISA, Protection du patrimoine informationnel, 30 novembre 2007.

***626. Les critères d'identification du secret des affaires au niveau européen et national.*** Pour pouvoir identifier « le secret des affaires » et prétendre, ainsi, à une protection légale contre l'obtention, la divulgation et l'utilisation illicites, il faut prendre en compte la nature de l'information et son origine[1478]. Concernant la nature des informations, la directive européenne impose les conditions suivantes[1479]: elles doivent être « secrètes », c'est-à-dire qu'elles ne sont pas connues et ne sont pas accessibles aux tiers[1480] ; elles doivent avoir une valeur commerciale parce qu'elles sont secrètes[1481] ; elles doivent faire l'objet, de la part du titulaire qui en a le contrôle, de dispositifs à les garder secrètes[1482]. Ensuite, concernant l'origine de l'information, il est exigé que le détenteur puisse justifier, du caractère licite du secret d'affaires, et donc de la source de son information d'affaires afin de pouvoir bénéficier du régime de protection. À ce titre, l'obtention d'un secret d'affaires est considérée comme licite lorsque « le secret d'affaires est obtenu par une découverte ou une création indépendante ; l'observation, l'étude, le démontage ou le test d'un produit ou d'un objet qui a été mis à la disposition du public ou qui est de façon licite en possession de la personne qui obtient l'information (…) et toute autre pratique qui (…) est conforme aux usages honnêtes en matière commerciale »[1483]. La transposition de cette Directive européenne de 2016 [1484] en droit interne est intervenue par la loi du 30 juillet 2018[1485], laquelle a instauré au profit des entreprises un régime spécifique permettant aux entreprises de se protéger contre une appropriation illicite de leur savoir-faire et de leurs informations commerciales et technologiques. Cette loi reprend la définition et les critères du « secret des affaires » inscrits dans la Directive européenne. Il s'agit des informations caractérisées par le caractère secret, disposant d'une valeur commerciale et ayant fait l'objet de dispositions destinées à les garder secrètes [1486]. À partir de ces dispositions, il est possible de définir que les secrets d'affaires correspondent aux renseignements confidentiels ayant une valeur économique et faisant l'objet de mesures de protection destinées à les garder secrets.

---

[1478] Binctin N., Répertoire IP/IT et Communication- Savoir-faire, Janvier 2018.

[1479] Directive européenne n° 2016/943 du Parlement européen et du Conseil du 8 juin 2016, *op. cit.*.

[1480] Définition du secret issue du règlement n°316/2014.

[1481] Binctin N., Répertoire IP/IT et Communication- Savoir-faire, Janvier 2018.

[1482] Directive européenne n° 2016/943 du Parlement européen et du Conseil du 8 juin 2016, *op. cit.*.

[1483] V. art. 3 de la Directive européenne n° 2016/943 du Parlement européen et du Conseil du 8 juin 2016, *op. cit.*.

[1484] Directive européenne n° 2016/943 du Parlement européen et du Conseil du 8 juin 2016, *op. cit.*.

[1485] Loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires, publiée au JORF n°0174 du 31 juillet 2018.

[1486] Gouache J-B., le secret des affaires : une nouvelle loi modifie le code de commerce, 2 octobre 2018 https://www.gouache.fr/articles/Articles/La-vie-du-franchiseur/Concurrence/Autre/Secret-des-affaires-une-nouvelle-loi-modifie-le-code-de-commerce.

***627. Les critères de qualification du « secret des affaires » à l'international.*** À l'international les secrets d'affaires sont, aussi, protégés. L'accord APIC[1487] affirme le principe de la protection du secret des affaires ainsi que les conditions des secrets d'affaires, lesquelles sont identiques à celles de la directive précitée[1488]. En effet, cet accord affirme le droit des personnes morales d'empêcher que des renseignements licitement sous leur contrôle ne soient divulgués à des tiers ou acquis ou utilisé par eux sans leur consentement et d'une manière contraire aux usages commerciaux honnêtes » à la condition que ces informations soient secrètes, disposent d'une valeur commerciale et ont fait l'objet de dispositions pour les garder secrètes[1489]. Quant aux États-Unis, la loi fédérale dénommée « Economic Espionage Act » ou « Cohen Act » a choisi de définir plus largement le secret des affaires comme « toute forme ou tout type d'information financière, commerciale, scientifique, technique, économique, industrielle, incluant modèles, plans, compilations, mécanismes, formules, dessins, prototypes, méthodes, techniques, procédés, procédures, programmes ou codes qu'elle se présente sous forme matérielle ou immatérielle qu'elle soit ou non stockée, compilée, ou mémorisée physiquement, économiquement, graphiquement, ou par écrit »[1490]. Les États-Unis ont choisi d'opter pour une définition large de la notion du « secret des affaires » afin d'étendre le plus possible la protection du secret des affaires des entreprises américaines ; alors qu'en France, on constate que la notion est plus cadrée.

***628. La détermination du secret des affaires***. Les secrets d'affaires sont définis, par la doctrine, comme étant « toutes les informations détenues par une entreprise qui, n'étant pas (nécessairement) connues des autres entreprises opérant sur le même marché, sont susceptibles de procurer à leur détenteur un avantage concurrentiel » et englobent « le secret de fabrique, les informations de nature «commerciale» ou «financière» (…): étude de marché, plan d'affectation du personnel, renseignements divers relatifs à la clientèle ou aux fournisseurs de l'entreprise (noms et données de contact, mais aussi, le cas échéant, informations quant aux transactions conclues et aux conditions contractuelles particulières accordées : prix, ristournes, quantités achetées, date d'expiration de garanties, profils d'investissement...), etc. » [1491]. Il peut s'agir de concepts commerciaux ou techniques, d'informations « négatives » (…) de logiciels, en particulier de codes-source et de la documentation qui s'y rapporte, de dossiers de fabrication, de méthodes d'essais, de données

[1487] Texte de l'Organisation Mondiale du Commerce (OMC), ADPIC (Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce), signé à Marrakech, au Maroc, le 15 avril 1994.

[1488] Directive européenne n° 2016/943 du Parlement européen et du Conseil du 8 juin 2016, *op. cit.*.

[1489] V. art. 39-2 de l'accord ADPIC.

[1490] La loi fédérale dénommée « Economic Espionage Act » du 11 octobre 1996 ou « Cohen Act » définit largement le secret des affaires : http://www.economicespionage.com/EEA.html.

[1491] Vanbrabant B., Les contrats relatifs au savoir-faire et autres secrets d'affaire, dans Secrets d'affaires, 113, les dossiers du journal des tribunaux (sous la direction de Vincent Cassiers), Larcier, édition 2020.

d'essais de matériaux ou de produits (…) d'informations technico-commerciales concernant des fournisseurs ou des clients »[1492].

***629.*** En sus de la consécration dans les textes du secret des affaires permettant un élargissement de la protection à l'ensemble des données confidentielles de la personne morale, il est adjoint des mesures contribuant, ainsi, à renforcer l'effectivité du droit au secret des affaires.

**2) Les mesures protectrices du patrimoine informationnel**

***630.*** La consécration du secret des affaires a permis d'établir diverses mesures légales pour renforcer la protection des données confidentielles des personnes morales. En sus de ces mesures légales, il est proposé de renforcer ces dispositifs légaux en les inscrivant à travers des dispositions spécifiques dans le contrat cloud.

***631.*** **Plan.** Nous aborderons, les mesures issues de la loi (a) et celles prévues par contrat (b).

a) Les mesures de protection issues de la loi

***632.*** Les mesures pour renforcer la protection des données confidentielles des personnes morales sont issues de la loi précitée de 2018 sur la protection du secret des affaires, laquelle a été suivie d'un décret d'application du 11 décembre 2018[1493]. Ce décret confère aux juges des pouvoirs étendus pour prévenir ou faire cesser une atteinte au secret des affaires et permet, ainsi, aux entreprises de renforcer la protection de leur savoir-faire ou de leurs informations commerciales et technologiques contre une appropriation illicite. Par la consécration de ce nouveau régime de protection du secret des affaires[1494], les données numériques stockées dans le cloud qui contiennent des informations confidentielles se trouvent protégées dès lors qu'elles remplissent les critères du « secret des affaires », c'est-à-dire, qu'il s'agisse de données secrètes, disposant d'une valeur commerciale et ont fait l'objet de dispositions raisonnables destinées à les rendre secrètes[1495]. En cas d'atteinte au secret des affaires par le prestataire de services cloud, dans le cadre de l'exécution d'un contrat de cloud computing, le client, personne morale, peut engager à son encontre une action en responsabilité fondée sur l'atteinte au secret d'affaires[1496]. Outre l'engagement de la

[1492] Hagel F., Secret et droits de propriété intellectuelle : un tour d'horizon, RLDI 10/2009, n° 53.

[1493] Décret n° 2018-1126 du 11 décembre 2018 relatif à la protection du secret des affaires.

[1494] Loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires, publiée au JORF n°0174 du 31 juillet 2018.

[1495] V. *supra* n°618 et suivants.

[1496] V. art. L.152-2 C. com.

responsabilité du prestataire qui sera abordée plus en détail dans la partie suivante dédiée aux voies de recours[1497], la loi a prévu un mécanisme permettant de prévenir (ou faire cesser) l'atteinte au secret des affaires afin de renforcer la protection des données des personnes morales. Ce mécanisme préventif permet, à la demande du client, personne morale, de demander au juge d'ordonner diverses mesures telles que l'interdiction des actes d'utilisation ou de divulgation d'un secret des affaires[1498]. Il s'agit d'une procédure d'urgence, et constitue une mesure provisoire et conservatoire afin de prévenir une atteinte imminente au secret des affaires ou à faire cesser une atteinte actuelle au secret des affaires[1499]. À titre de renforcement de la protection des données des personnes morales, il est prévu un mécanisme de garanties[1500] permettant au juge d'ordonner la constitution de garanties soit par le demandeur ayant obtenu l'octroi de mesures provisoires ou conservatoires si l'atteinte au secret était jugée par la suite comme infondée et ainsi permettre l'indemnisation du défendeur ou d'un tiers concerné par les mesures, soit par le défendeur, comme condition pour l'autoriser à poursuivre l'utilisation illicite alléguée et ainsi prévoir l'indemnisation du demandeur à la protection du secret des affaires. Ce type de mesure permet au client, personne morale, dans le cadre de l'exécution du contrat de cloud computing, d'obtenir du juge des mesures immédiates de protection de ses données renfermant un secret des affaires avec la contrepartie de constituer une garantie. Il s'agit, donc, d'un mécanisme à l'avantage du client, personne morale puisque soit le juge fait droit à sa demande de protection de ses données couvertes par le secret en contrepartie de la constitution d'une garantie soit il décide de ne pas accéder à sa demande, mais demande au prestataire de services cloud de constituer une garantie. Dans les deux hypothèses, la donnée constituant un secret d'affaires est soit préservée par l'établissement d'une mesure préventive, soit protégée par la constitution d'une garantie au profit du client, personne morale.

***633.*** À cette mesure préventive, il est ajouté la possibilité pour le client, personne morale, de demander aux juges d'ordonner d'office le placement sous séquestre « provisoire » des documents obtenus dans le cadre d'une mesure d'instruction in futurum ou d'une saisie-contrefaçon afin d'assurer la protection du secret des affaires[1501]. Ce type de mesure contribue, aussi, à préserver le caractère confidentiel des données de la personne morale. La préservation de la confidentialité des données est renforcée par la mise en place de mesures d'ordre procédural. À ce titre, il est prévu la possibilité de demander la confidentialité du jugement afin de préserver que la donnée secrète des affaires ne soit pas divulguée dans la publication du jugement. À ce titre, le client, personne morale, a la possibilité de demander au juge un extrait de la décision ne comportant que son dispositif,

[1497] V. *infra* n° 635 et suivants.

[1498] V. art. L.152-3-1 C. com.

[1499] V. art. R.152-1 C. com.

[1500] V. art. R.152-1 I et III C. com.

[1501] V. art. R.153-1 C. Ccom.

revêtu de la formule exécutoire qui pourra lui être remise pour les besoins de son exécution forcée, et que dans une version destinée à être publiée ou diffusée que les informations couvertes par le secret des affaires soient occultées[1502]. En revanche, il existe un risque de divulgation des informations jugées sensibles et confidentielles au grand public en cas de refus d'un huis clos par le juge. Afin de se prémunir contre un tel risque de divulgation, il serait opportun d'envisager la voie de l'arbitrage, qui se veut confidentiel et laquelle sera contractuellement encadrée.

***634.*** Si la consécration du secret des affaires et l'établissement de ces mesures légales permettent de renforcer la protection des données confidentielles des personnes morales, il est nécessaire d'adjoindre à celles-ci des mesures contractuelles.

b) Les mesures de protection prévues par le contrat cloud

***635. Le renforcement de la protection du secret des affaires dans le contrat de cloud computing.*** En sus des mesures légales, il est proposé de renforcer les données couvertes par le secret des affaires par des clauses spécifiques, telles que la clause de confidentialité ou d'annexer au contrat de cloud computing, un accord de confidentialité[1503], ou un accord de secret.

***636.*** Il est proposé ci-après une rédaction d'un accord de secret adapté à la protection des données confidentielles dans le cadre de l'exécution d'un contrat de cloud computing.

### *637.* ACCORD DE PROTECTION DES DONNÉES DU SECRET D'AFFAIRES ANNEXE AU CONTRAT DE CLOUD COMPUTING

entre

**.....,** société ..... *(forme de la société)*, ayant son siège social ..... *(adresse du siège social)*, enregistrée au Registre du Commerce et des Sociétés de ..... *(localité du RCS)*, sous le numéro ..... *(n° RCS)*, représentée par M. / Mme..... (nom du représentant), ..... *(qualité du représentant)*, dûment habilité à l'effet des présentes,

ci-après désigné(e) par **« le Prestataire »,**

**D'UNE PART,**

[1502] V. art. R.153-10 C. com. V. également, les art.R.153-2's et art L.153-1 C. com relatifs aux règles procédurales lors d'une demande de communication ou de production de pièces.

[1503] V. *infra* n° 665.

**ET**

**.....,** société ..... *(forme de la société)*, ayant son siège social ..... *(adresse du siège social)*, enregistrée au Registre du Commerce et des Sociétés de ..... *(localité du RCS),* sous le numéro ..... *(n° RCS)*, représentée par M. / Mme ..... (nom du représentant), ..... *(qualité du représentant),* dûment habilité à l'effet des présentes,

ci-après désigné(e) par **« le Client »,**

**D'AUTRE PART,**

**PRÉAMBULE**

Dans le cadre de la conclusion d'un contrat de cloud computing, les Parties acceptent d'annexer au contrat de cloud computing (ci-après désigné contrat principal), le présent accord relatif à la protection des données du secret d'affaires.

Afin de protéger les informations confidentielles du Client couvertes par le secret des affaires, les Parties ont l'intention de s'engager juridiquement et sont convenues de ce qui suit :

**Article 1 - Définitions**

**1.1** Le terme « DONNÉE(S) », désigne les informations de toute nature détenues par le Client incluant de manière non limitative : le savoir -faire, le secret de fabrique, les informations de nature commerciale (étude de marché, portefeuille client et fournisseur de l'entreprise…), financière (informations sur le chiffre d'affaires, bénéfices, pertes ), contractuelle (conditions particulières accordées telles que les prix, ristournes, quantités achetées, date d'expiration de garanties...), marketing (stratégies de communication et de développement, procédés et outils marketing utilisés), technique (procédés techniques de développement des produits, logiciel, code-source..) et plus généralement, toute documentation sous format électronique s'y rapportant.

**1.2** Le terme « Secret d'affaires » désigne la protection offerte par la loi concernant les DONNÉES confidentielles des personnes morales ayant une valeur économique et faisant l'objet de mesures de protection destinées à les garder secrètes.

Ces DONNÉES constituent l'objet du présent accord et seront ainsi tenues pour confidentielles.

**Article 2 – Objet**

L'accord a pour objet de fixer les règles relatives à la protection de la DONNÉE du Client hébergée dans l'infrastructure en nuage du Prestataire.

**Article 3 – Déclarations du Client**

Le Client déclare qu'il bénéficie d'un droit de propriété exclusif sur sa DONNÉE et n'accorder, au Prestataire, aucun droit sur sa DONNÉE.

**Article 4 - Obligations du Prestataire**

**4.1** Le Prestataire s'engage à ne pas accéder, à utiliser, traiter, exploiter la DONNÉE, appartenant exclusivement au Client, hébergée dans les serveurs de son infrastructure en nuage.

**4.2** Le Prestataire s'engage à ne pas troubler la jouissance paisible du droit de propriété du Client sur sa DONNÉE et s'interdit de réaliser une quelconque action ou manipulation technique sur la DONNÉE de son Client, entendu largement et de manière non limitative comme : toute utilisation, toute duplication, tout traitement, toute exploitation, toute représentation, toute reproduction et toute transmission.

**4.3** Le Prestataire s'engage à ne communiquer la DONNÉE appartenant au Client à aucune personne ou entité et à prendre toutes mesures nécessaires pour éviter que son personnel ne divulgue à des tiers tout ou partie de la DONNÉE.

**Article 5 – Propriété des données**

**5.1** Le Client demeure le propriétaire exclusif de la DONNÉE hébergée dans les serveurs de l'infrastructure en nuage du Prestataire.

**5.2** Le présent Accord n'autorise aucun transfert de propriété´ au profit du Prestataire.

**5.3** Le présent Accord ne peut, en aucun cas, être interprété comme conférant de manière implicite une concession de licence de brevet, de marque ou d'autres droits de propriété intellectuelle ou industrielle reconnus par la loi.

**Article 6 – Responsabilité**

En cas de contravention à l'une des dispositions du présent Accord et plus généralement d'une atteinte à la protection des DONNÉES du secret d'affaires, le Prestataire s'engage à réparer l'intégralité des préjudices qui résulteront de cette atteinte sans opposer une quelconque limitation de responsabilité dès lors que l'atteinte est avérée et lui est imputable.

**Article 6 – Durée**

L'Accord entre en vigueur à compter de la date de signature du contrat principal par les Parties et est conclu pour la durée de validité du contrat principal.

**Article 7 – Résiliation**

L'accord ne peut être résilié indépendamment de la résiliation du contrat principal signé entre les Parties.

**Article 9 – Litiges et droit applicable.**

**9.1** Le présent accord est soumis à la réglementation française en vigueur.

**9.2** En cas de contestation, les Parties peuvent décider, individuellement ou collectivement, de mandater un expert aux fins de constatations, de délimitation du champ de l'atteinte aux droits du Client sur sa DONNÉE et de détermination de l'étendue du préjudice réparable.

**9.3** En cas de désaccord, les Parties s'engagent, en priorité, à privilégier la résolution du litige à l'amiable avant tout recours contentieux.

**9.4** En cas de contestation persistante, les Parties acceptent de soumettre leur différend aux juridictions françaises compétentes.

Fait le ..... *(date),* A ..... *(lieu),*

En deux exemplaires originaux,

Pour le Prestataire (signature)

Pour le Client (signature)

***638.*** Il en résulte que la consécration du secret des affaires accompagnée des dispositifs légaux de prévention ainsi que l'intégration dans le champ contractuel de la préservation du secret des affaires permettent de renforcer la protection du patrimoine informationnel de la personne morale.

***639.*** Outre l'élargissement du champ de la protection à l'ensemble des données d'affaires et de l'établissement de mesures spécifiques de protection, la consécration du secret d'affaires permet, également, d'élargir les voies d'actions existantes en matière de responsabilité délictuelle.

## B) le renforcement de la protection par un élargissement de la responsabilité délictuelle

***640.*** Cette partie est consacrée à l'étude de la protection des données des personnes morales dans le cadre de l'exécution d'un contrat de cloud computing. Le renforcement de la protection des données confidentielles de la personne morale est rendu possible par un élargissement des actions en responsabilité délictuelle au profit du Client. Qu'il s'agisse du prestataire de services cloud ou de son sous-traitant, la loi prévoit des actions de nature civile et pénale ouvertes à la personne morale victime de la divulgation de ses données confidentielles dans le cadre de l'exécution d'un contrat de cloud computing. Ces actions sont ouvertes sous la réserve de remplir les conditions exigées par les textes.

***641.*** **Plan.** Il est question d'étudier, de manière distincte, les responsabilités civiles (1) et les responsabilités pénales (2) exercées à l'encontre du prestataire de services cloud et/ou de son sous-traitant.

**1) La mise en œuvre des responsabilités civiles dans le cadre de l'exécution d'un contrat cloud**

***642. L'application de l'action civile en concurrence déloyale au contrat cloud.*** L'action en concurrence déloyale est d'origine doctrinale et jurisprudentielle et est fondée sur les articles 1240 et 1241 du Code civil (anciens articles 1382 et 1383). La concurrence déloyale est « le fait, dans le cadre d'une concurrence autorisée, de faire un usage excessif de sa liberté d'entreprendre, en recourant à des procédés contraires aux règles et usages, occasionnant un préjudice »[1504]. Il s'agit, donc, d'un comportement contraire à la morale des affaires et contribue à fausser le jeu de la libre concurrence ». Ces pratiques comportementales ont pour objet de nuire à une entreprise concurrente. La question se pose de savoir si ce type d'action est envisageable alors même que le client et le prestataire de services ne sont pas des concurrents directs. À cette question, la chambre commerciale de la Cour de cassation dans son arrêt en date du 3 mai 2016 est venue préciser « qu'une situation de concurrence directe ou effective entre les sociétés considérées n'est pas une condition de l'action en concurrence déloyale qui exige seulement l'existence de faits fautifs générateurs d'un préjudice »[1505]. Il en résulte de cette décision que la situation d'une concurrence directe ou effective entre les personnes morales (ici entre le client et le prestataire de services cloud) n'est pas une condition prévue par la loi pour engager une action sur le fondement de l'action en concurrence déloyale. L'action en concurrence déloyale correspond à une variété de la responsabilité civile délictuelle dont le principe est que toute personne qui cause un préjudice à autrui soit par sa faute, soit par sa négligence en doit réparation[1506]. Cette action peut, donc, être envisagée dès lors que la victime de la divulgation d'une donnée confidentielle ne peut pas s'appuyer sur des droits privatifs[1507]. À titre illustratif, il apparaît que l'action en concurrence déloyale a pu être admise par les juges à titre subsidiaire lorsque l'action sur le fondement du droit sui generis échouait en raison du défaut des conditions exigées relatives à l'investissement substantiel[1508]. De même, l'action en concurrence déloyale est utilisée dans le cadre d'une exploitation abusive du savoir-faire d'autrui[1509]. Cette action civile de droit commun, issue du régime de la responsabilité délictuelle[1510], exige que la victime démontre le fait dommageable, le préjudice et le lien de

[1504] Définition concurrence déloyale, fiches d'orientation, Dalloz, juin 2021.

[1505] Cass. com. 3 mai 2016, pourvoi n°14-24905.

[1506] V. art. 1240 et 1241 C. civ.

[1507] V. *infra* n° 635.

[1508] V. CA Rennes, 23 janv. 2018, affaire n° 15/06101.

[1509] Ledoux P., 1679 - Recours au droit commun de la responsabilité, Le Lamy droit commercial, mis à jour 04/2022.

[1510] L'action en concurrence déloyale est d'origine doctrinale et jurisprudentielle et est fondée sur les articles 1240 et 1241 du Code civil (anciens articles 1382 et 1383). Il s'agit d'une variété de la responsabilité civile dont le principe est que toute personne qui cause un préjudice à autrui soit par sa faute, soit par sa négligence en doit réparation. L'article 1240 du Code civil (ancien article 1382) : «

causalité. Quels peuvent être ces procédés concurrentiels déloyaux et est-ce qu'ils sont applicables en matière de cloud computing ? C'est le Doyen Roubier qui a établi une classification en quatre catégories que sont les moyens de confusion, le dénigrement, la désorganisation interne d'une entreprise rivale et la désorganisation générale du marché[1511]. Puis Monsieur Saint-Gal a ajouté le cas du parasitisme[1512]. Dans le cadre de l'exécution du contrat de cloud computing, la divulgation du secret des affaires est rattachée à la notion de désorganisation interne de l'entreprise, sous forme de détournement de données (de fichiers). Pour que cette action en concurrence déloyale soit recevable encore faut-il démontrer que le destinataire du secret divulgué l'ait exploité à son profit. À titre d'exemple, les juges ont sanctionné, sur le fondement d'une action en concurrence déloyale, le détournement de fichiers (liste de clients, liste de fournisseurs…)[1513]. La cour de cassation concernant la responsabilité civile a admis la présomption du préjudice en matière de concurrence déloyale et de parasitisme[1514]. Cette présomption de préjudice « permet d'écarter toute difficulté probatoire pour des effets préjudiciables dont la preuve est délicate à rapporter pour le demandeur (..) et la restauration de l'équilibre entre concurrents »[1515]. Afin d'éviter que les recours juridictionnels contribuent à la divulgation du secret des affaires au public, il est possible de demander que les procès soient réalisés à huis clos et même envisager de recourir à la voie de l'arbitrage.

***643.*** Par ailleurs, la question s'est posée de savoir s'il était possible de cumuler deux actions, dont l'une serait fondée sur un droit privatif, tel que l'atteinte au droit sui generis du producteur de la base de données et l'autre sur une concurrence déloyale. Au niveau de la doctrine, les positions divergent concernant la possibilité de cumuler ces deux actions[1516]. À la différence, la jurisprudence a admis que l'action en concurrence déloyale puisse être exercée « à titre complémentaire lorsque les faits invoqués (risque de confusion à l'égard des tiers, démarchage déloyal, détournement déloyal de clientèle) sont distincts de ceux permettant de caractériser

---

Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer » ; L'article 1241 du Code civil (ancien article 1383) : « Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence ». Au succès de cette action, il faudra apporter la preuve d'une faute, d'un préjudice et un lien de causalité.

[1511] Roubier P., « Le droit de la propriété industrielle », t. I, éd. Sirey, 1952, n° 110

[1512] Saint-Gal Y., « Concurrence déloyale et concurrence parasitaire », RIPIA, 1956, p. 37 ; « Protection et défense des marques de fabrique et concurrence déloyale, 5ème éd., Delmas, 1982.

[1513] Cass. Crim 9 septembre 2003, pourvoi n°02-87.098, inédit.

[1514] Cass. com., 17 mars 2021, n° 19-10.414, inédit : JurisData n° 2021-003856.

[1515] Mendoza-Caminade A., La présomption de préjudice en matière de concurrence déloyale et de parasitisme, La Semaine Juridique Edition Générale n° 22, 31 mai 2021, act. 581.

[1516] En faveur du cumul, Mallet-Poujol N., Protection des bases de données, J-Cl. Communication, fasc. 6080, 2010, spéc. n° 194 ; Contre le cumul, Passa J., Responsabilité civile. Concurrence, PI 2002, n° 5, p. 107 ; P.-Y. Gautier, Propriété littéraire et artistique, 8e éd., PUF, 2012, n° 183.

l'atteinte du droit *sui generis*[1517] »[1518]. Il a, également, été considéré que le producteur de la base de données peut toujours invoquer la concurrence déloyale ou le parasitisme[1519], soit de manière complémentaire, soit de manière autonome au droit d'auteur et/ou au droit sui generis[1520]. Ces droits viennent sanctionner un comportement fautif[1521]. À titre illustratif, les juges du fond ont considéré que « le parasitisme est caractérisé par la circonstance selon laquelle une personne, à titre lucratif et de façon injustifiée, s'inspire ou copie la valeur économique d'autrui, individualisée et procurant un avantage concurrentiel, fruit d'un savoir-faire, d'un travail intellectuel et d'investissements »[1522]. Qu'il s'agisse de l'action fondée sur la concurrence déloyale ou plus spécifiquement sur le parasitisme, ces actions peuvent être entreprises par le client à l'encontre de son prestataire de services cloud si un des comportements déloyaux lui est imputable. L'intérêt pour le client, d'exercer une action en concurrence déloyale contre le prestataire de services cloud, est de demander aux juges, dans le cadre d'une procédure en référé, la cessation des agissements du Prestataire constitutifs d'une concurrence déloyale dans les plus brefs délais. Également, le Client, en exerçant cette action, pourra obtenir des dommages et intérêts à titre de réparation des préjudices subis.

***644. L'application de l'action civile en contrefaçon au contrat de cloud computing.*** En matière de cloud, la donnée est immatérielle ; en conséquence la protection de l'œuvre dématérialisée par le droit d'auteur oblige, « le numérique oblige à repenser les territoires des monopoles et les moyens de lutte contre la contrefaçon »[1523]. En effet, la commission d'un délit de contrefaçon s'en trouve facilité par la facilité de la reproduction immatérielle et de la circulation de l'œuvre en dehors du territoire national du créateur[1524]. L'action en contrefaçon est conditionnée à une atteinte à un droit de propriété intellectuelle (un droit privatif). Tel qu'il a été abordé dans la partie ci-dessus[1525], le patrimoine informationnel du client, personne morale, peut renfermer des données protégées par des droits privatifs tels qu'un droit sui generis du producteur de la base

[1517] V. par ex., pour des faits de démarchage déloyal, Paris, 21 nov. 2008, Juris-Data n° 2008-373507 ; Propr. ind. 2009. Comm. 30, obs. J. Larrieu.

[1518] Chatry S., La légitimité du droit sui generis du producteur de bases de données, Légipresse 2019.

[1519] Lequel correspond à une catégorie spécifique de la concurrence déloyale établie par M. Y. Saint-Gal : v. *supra* n° 635 et suivants.

[1520] Costes L., Perray R., Adda H. sous la direction de Costes L., Le Lamy droit du numérique (Guide), Partie 6 - Guide, Titre 5 Comment exploiter les bases de données et les créations multimédia ? Chapitre 3 Protection de l'ensemble informationnel, Section 2 Protection des bases de données, § 3. Protection par l'action en concurrence déloyale et en parasitisme, mis à jour 04/2022.

[1521] V. *supra* n° 591 et suivants (droit sui generis).

[1522] CA Paris, 1re ch., 25 nov. 2009, SARL Paris-Paris c/ Marant.

[1523] Gleize B., et Maffre-Baugé A., La propriété intellectuelle renouvelée par le numérique, édition Dalloz, Collection Thèmes et Commentaires, novembre 2020.

[1524] V. *infra* n° 686 et suivants (l'extraterritorialité).

[1525] V. *supra* n° 573 et suivants (patrimoine informationnel).

de données, un droit d'auteur sur l'architecture de la base de données[1526], un droit d'auteur sur les œuvres de l'esprit, un droit de marque, un brevet (..). À ce titre, si la donnée immatérielle dans le cloud computing constitue une œuvre d'esprit[1527], elle pourra être protégée par le droit d'auteur et toute atteinte à ce droit est sanctionnable par le délit de contrefaçon[1528]. Afin de garantir au Client, personne morale, dans le cadre d'un contrat de cloud computing, à une exclusivité d'exploitation de ses œuvres dématérialisées[1529], la sanction du délit de contrefaçon doit pouvoir s'appliquer en cas d'atteinte.

***645.*** Au choix du demandeur, bénéficiaire d'un droit privatif, l'action en contrefaçon[1530] peut être engagée dans le cadre d'une procédure civile et pénale[1531]. En la matière, la preuve est libre [1532] et peut faire l'objet en amont d'une saisie-contrefaçon[1533]. La question se pose de savoir, si le client, personne morale, peut agir contre le Prestataire de services dès lors qu'il a porté atteinte à son droit de propriété intellectuelle ou industrielle. La qualité à agir a été débattue, en raison que les textes prévoient la protection par le droit de la propriété intellectuelle uniquement au créateur, personne physique, et le droit de la propriété industrielle, uniquement à l'inventeur, personne physique. S'il est admis que la titularité d'un droit de propriété intellectuelle ou industrielle ne peut pas être accordée à la personne morale[1534], il en est différent lorsqu'il s'agit de trancher la question de la qualité à agir. La jurisprudence est constante depuis un arrêt de la 1re chambre civile de la Cour de cassation qui admet que la personne morale puisse avoir la qualité à agir pour exercer une action en contrefaçon[1535]. Il en résulte que le client, personne morale, a la qualité pour exercer une action en contrefaçon contre son prestataire de services qui a porté atteinte à un droit de la propriété intellectuelle ou industrielle.

***646.*** Concernant les sanctions civiles, il s'agit de condamner l'auteur de l'atteinte au paiement de dommages et intérêts. À titre illustratif, en matière d'atteinte à une donnée protégée par le droit d'auteur, le client, personne morale, peut obtenir de son prestataire de services cloud (auteur des

---

[1526] Vivant M., « La contrefaçon entre contrat et délit, Réflexion sur les catégories juridique » Mélanges en l'honneur du professeur Jacques Mestre, LGDJ, 2019, p. 931.

[1527] V. *supra* n° 605 et suivants (droit d'auteur).

[1528] V. art. L.335-2's du CPI.

[1529] Bitan H., Droit et expertise du numérique, Créations immatérielles, Données personnelles, E.réputation, Droit à l'oubli, Neutralité, Responsabilité civile et pénale, *op. cit*..

[1530] Délit de contrefaçon : v. art. L335-2's CPI.

[1531] Marcellin, Y. « La protection pénale de la contrefaçon de marques et de dessins et modèles », RDPI 1996 no 63 p. 24

[1532] V. art. L332-4 du CPI relatif à la preuve libre concernant la contrefaçon de logiciels et de bases de données. Également, v. art. 427 CPI. V. également, Cass. crim., 5 septembre 1989, pourvoi n° 88-83470, CNC c/ Consorts Sudre, RTD Com. 1990 p.388 ; Rida n° 144 avr. 1990, p. 201, concernant l'administration de la preuve par le juge.

[1533] V. art. L332-4 CPI relatif à la saisie des logiciels et des données prétendument contrefaisants.

[1534] V. *supra* n° 608 relatif à la confrontation de la théorie personnaliste du droit d'auteur à la théorie réaliste (qui se veut pragmatique et fondée sur l'économie).

[1535] Cass. 1re civ., 24 mars 1993, 2e espèce, JCP G 1993, II, no 22085, note Greffe P., RIDA 1993, no 158, p. 200. V. également, Cass. 1re civ., 3 juill. 1996, JCP E 1997, I, no 657, no 5, obs. Vivant M. et Le Stanc Ch., D. 1997, jur., p. 328, note Françon.

dommages), une allocation de dommages et intérêts. Concernant la fixation du montant des dommages et intérêts, il est précisé à l'article L331-1-3 du CPI que « la juridiction prend en considération distinctement :les conséquences économiques négatives de l'atteinte aux droits, dont le manque à gagner et la perte subis par la partie lésée ; le préjudice moral causé à cette dernière ; et les bénéfices réalisés par l'auteur de l'atteinte aux droits, y compris les économies d'investissements intellectuels, matériels et promotionnels que celui-ci a retirées de l'atteinte aux droits ». Cette disposition légale permet d'élargir le champ de la réparation et ainsi renforcer la protection des œuvres d'esprit dématérialisées du client, personne morale[1536]. En outre, il est précisé que le juge se réserve la possibilité d'ordonner « toute mesure appropriée de publicité de jugement »[1537], cette mesure peut avoir des conséquences importantes en termes d'image pour le contrefacteur. La personne morale ne pourra pas agir en contrefaçon lorsque la donnée concernée est une information confidentielle relative, par exemple, à la stratégie de l'entreprise sur le marché, aux données économiques et financières. Dans ce cas de figure, il s'agit de s'orienter vers l'action spéciale relative au secret des affaires.

***647. La responsabilité civile spéciale pour atteinte au secret des affaires.*** Dans ce contexte, le législateur, conscient des lacunes légales en matière de protection des données confidentielles des personnes morales, a été adopté par la loi du 30 juillet 2018[1538] pour protéger le secret d'affaires et permettre, ainsi, d'engager la responsabilité de(s) auteur(s). Il est intéressant de s'interroger sur l'impact de cette loi quant à la protection des données confidentielles de la personne morale dans les contrats de cloud computing. En effet, pendant de très nombreuses années, il n'existait pas de texte réprimant la divulgation de ces données sensibles des personnes morales et le stratagème était de passer par des voies de droits ordinaires[1539]. La protection des données confidentielles des personnes morales a connu un renforcement par la consécration par la loi du 30 juillet 2018, du droit au « secret des affaires » qui permet d'engager la responsabilité des acteurs qui sont à l'origine de l'atteinte au droit du secret des affaires » dont le délai de prescription est fixé à 5 ans[1540]. Il s'agit d'une responsabilité civile spéciale prévue à l'article L152-1 et suivant du code de commerce qui dispose que « toute atteinte au secret des affaires comme prévu aux articles L. 151-4 à L. 151-6 engage la responsabilité civile de son auteur ». En

[1536] Vivant M., « La contrefaçon entre contrat et délit, Réflexion sur les catégories juridique » Mélanges en l'honneur du professeur Jacques Mestre, LGDJ, 2019, p. 931.

[1537] V. art. L331-1-4 du CPI.

[1538] V. Loi n° 2018-670 du 30 juillet 2018.

[1539] Telles que les actions en contrefaçon, en concurrence déloyale, en violation des secrets de fabrique et éventuellement l'escroquerie.

[1540] V. art. L152-2 C. com, également, v. De Roux H., Zilberman A., La loi sur le secret des affaires : un premier élan vers la protection des données sensibles des entreprises françaises ? Revue Lamy droit des affaires, N° 141, 1er octobre 2018.

cas d'atteinte au secret des affaires par le prestataire de services cloud, dans le cadre de l'exécution d'un contrat de cloud computing, le client, personne morale, peut engager à son égard une action en responsabilité fondée sur l'atteinte au secret d'affaires[1541]. En l'occurrence, l'obtention du secret des affaires n'est illicite que lorsqu'elle est réalisée sans le consentement de son détenteur légitime, lui-même définit à l'article L.151-2 du code de commerce comme la personne qui a licitement le contrôle du secret[1542]. Ainsi, le prestataire de services cloud peut voir sa responsabilité engagée dès lors qu'il a obtenu, utilisé ou divulgué un secret d'affaires de manière illicite. L'article L151-4 précise les cas d'obtention illicite d'un secret d'affaires ; il peut s'agir d'un accès non autorisé à tout document, fichier numérique (..) qui contient le secret ou dont il peut en être déduit, ou bien d'une appropriation ou d'une copie non autorisée de ces éléments, ainsi que tout autre comportement considéré, comme déloyal et contraire aux usages en matière commerciale. Il apparaît que cette disposition a un champ explicitement large afin de couvrir le plus possible des cas d'obtention illicite d'un secret d'affaires. Outre l'obtention illicite d'un secret d'affaires, les articles L151-5 et L151-6 précisent, également, les cas d'utilisation ou de divulgation illicite d'un secret d'affaires de manière large afin de couvrir le plus possible des situations d'atteinte au secret des affaires. Il est précisé auxdits articles que « l'utilisation ou la divulgation d'un secret des affaires est illicite lorsqu'elle est réalisée sans le consentement de son détenteur légitime par une personne qui a obtenu le secret dans les conditions mentionnées à l'article L. 151-4 ou qui agit en violation d'une obligation de ne pas divulguer le secret ou de limiter son utilisation »[1543]. Cette disposition permet d'élargir la responsabilité délictuelle à l'atteinte au secret d'affaires qui serait constitué en violation d'une obligation contractuelle. Ces dispositions sont favorables aux clients qui, en cas de manquement par le prestataire à une obligation de non-exploitation de ses données confidentielles, pourront utiliser le fondement juridique de l'atteinte au secret des affaires pour engager sa responsabilité civile. L'objectif de cette action est de permettre au client, personne morale, de recevoir une indemnisation financière pour réparer les préjudices subis résultant de l'atteinte aux données hébergées dans le cloud computing, renfermant des secrets d'affaires. Pour renforcer cette proposition d'admission d'une responsabilité du prestataire fondée sur l'atteinte au secret, le Professeur Vivant a suggéré d'étendre la responsabilité du prestataire aux tiers « complices » : « Le débiteur du secret ( …) pourra être condamné s'il méconnaît son obligation, mais, au-delà, on pourra au mieux attendre la condamnation du complice »[1544]. Il préconise, ainsi, l'extension

[1541] V. art. L152-1 C. com.

[1542] Ledoux P., 1681 Détenteur légitime, Le Lamy droit commercial, mis à jour 04/2022

[1543] V. L.151-5 et L.151-6 C. com.

[1544] Vivant M., La privatisation de l'information par la propriété intellectuelle, dans Revue internationale de droit économique 2006/4 (t. XX, 4), pages 361 à 388.

de la responsabilité civile du prestataire aux tiers non-partis au contrat principal. Dorénavant, la loi prévoit la condamnation de toute personne ayant porté atteinte à une information couverte par le secret des affaires, peu importe si celle-ci entretient une relation contractuelle ou pas[1545]. Il est, ainsi, possible d'engager la responsabilité civile délictuelle de tout responsable (le prestataire, le sous-traitant et tout autre tiers au contrat) qui a causé des préjudices à la personne morale résultant d'une obtention, d'une utilisation ou d'une divulgation illicite de son secret d'affaires[1546]. En revanche, s'agissant des autres types de données non couvertes par le secret des affaires, telles que le nom commercial, l'enseigne, la dénomination sociale et le nom de domaine, la protection demeure assurée par le droit commun de la responsabilité civile fondée sur les articles 1240 et suivant du Code civil[1547].

***648. Une responsabilité spéciale à l'activité du cloud computing.*** S'agissant de l'application de la responsabilité de droit commun, le professeur Chantepie envisage que cette responsabilité puisse être complétée par une responsabilité spéciale issue de l'article 15-1 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique[1548], et ce en opérant une interprétation amplifiante[1549]. Cette disposition prévoit un cas de responsabilité de plein droit à l'égard de toute personne (physique ou morale) exerçant l'activité définie à l'article 14 de la loi à savoir : « une activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens et de services »[1550] « à l'égard de l'acheteur de la bonne exécution des obligations résultant du contrat, que ces obligations soient à exécuter par elle-même ou par d'autres prestataires de services, sans préjudice de son droit de recours contre ceux-ci. Toutefois, elle peut s'exonérer de tout ou partie de sa responsabilité en apportant la preuve que l'inexécution ou la mauvaise exécution du contrat est imputable, soit à l'acheteur, soit au fait, imprévisible et insurmontable, d'un tiers étranger à la fourniture des prestations prévues au contrat, soit à un cas de force majeure ». Si ce texte s'applique au prestataire de services cloud puisque rentrant dans la catégorie des acteurs du commerce électronique, un débat fut ouvert concernant les bénéficiaires[1551]. À la lecture de l'article 15-I, il apparaît que cette responsabilité de plein droit ne bénéficie qu'aux « acheteurs », ce qui entraîne une exclusion contestable « des clients ayant sollicité une prestation de services ». Le professeur

[1545] V. art. L.152-1 C. com.

[1546] V. *supra* n° 640 et suivants.

[1547] V. art.1240 C. civ. (ancien article 1382) et art. 1241 C. civ. (ancien article 1383)

[1548] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique dite LCEN.

[1549] Chantepie G., L'inexécution du contrat de cloud computing, RLDI, nº 98, 1er novembre 2013.

[1550] V. alinéa 1er de l'article 14 de la loi du 21 juin 2004, *op. cit.*.

[1551] V. Dionis du Séjour J., Rapport AN, nº 612, p. 16., dans Chantepie G., L'inexécution du contrat de cloud computing, RLDI, nº 98, 1er novembre 2013.

Chantepie indique à ce sujet que les débats parlementaires ont permis de comprendre « que la garantie a été conçue pour résoudre un problème propre à la vente à distance (décalage entre transfert de propriété et livraison)[1552]. Pour admettre cette responsabilité des prestataires de services de plein droit laquelle instaure une forme de « responsabilité du fait d'autrui »[1553], le Professeur suggère de procéder à « une interprétation amplifiante fondée sur la cohérence du dispositif (là où la raison de la loi est la même, la loi doit être la même) », en rappelant que l'article 15, II utilise le terme de « contrat » « plus accueillant, et qui aurait pu être repris directement dans la disposition jumelle » à savoir à l'article 15-I[1554]. Il en résulte que compte tenu de cette incertitude quant au sujet de l'admission de cette responsabilité de plein droit aux prestataires de services, la seule solution restante serait de prévoir l'intégration de cette responsabilité dans le contrat de cloud computing. Une rédaction de cette clause est proposée ci-après :

***649.*** ***«*** Le Prestataire est responsable de plein droit à l'égard du Client de la bonne exécution des obligations résultant du contrat, que ces obligations soient à exécuter par elle-même ou par son (ses) sous-traitant(s). Le Prestataire peut s'exonérer de tout ou partie de sa responsabilité en apportant la preuve que l'inexécution ou la mauvaise exécution du contrat est imputable soit au Client, soit au fait, imprévisible et insurmontable, d'un tiers étranger à la fourniture des prestations prévues au contrat, soit à un cas de force majeure ».

***650.*** S'il peut paraître opportun d'intégrer cette clause pour renforcer la protection des données confidentielles du Client, personne morale ; il est peu probable, en pratique, que le prestataire accepte d'entériner le contrat avec la présence de cette clause. Les actions en responsabilité civile ont pour objet de réparer le dommage et non de sanctionner les agissements préjudiciables. Très souvent, l'allocation des dommages et intérêts versée aux victimes de la divulgation du secret des affaires peut s'avérer insuffisante, car le dommage résidant dans la divulgation du secret cause un préjudicie irréversible, tel que la perte d'un client important ou d'un marché. Sur ce point, la doctrine considère que « le mécanisme de réparation intégrale de la responsabilité civile est incapable d'appréhender avec justesse les dommages potentiellement subis par une entreprise » dont les données confidentielles viennent d'être détournées par son partenaire contractuel ou sa concurrente[1555]. C'est par ce constat qu'il faudrait peut-être envisager la voie pénale afin au mieux de dissuader « les fournisseurs de services cloud » de

[1552] Ibid.

[1553] V. Bacache M., Les nouveaux défis du droit de la responsabilité : l'article 15 de la loi pour la confiance dans l'économie numérique consacre-t-il un nouveau cas de responsabilité contractuelle du fait d'autrui ? *in* Rochfeld J. (ss dir.), Les nouveaux défis du commerce électronique, précité, p. 31, n° 33.

[1554] Chantepie G., L'inexécution du contrat de cloud computing, RLDI, n° 98, 1er novembre 2013.

[1555] De Roux H., Zilberman A., La loi sur le secret des affaires : un premier élan vers la protection des données sensibles des entreprises françaises ? Revue Lamy droit des affaires, N° 141, 1er octobre 2018.

divulguer des informations confidentielles de leurs clients. À côté des actions civiles, la personne morale de droit privé victime de la divulgation de ses données confidentielles a, donc, la faculté d'engager des actions pénales contre les auteurs présumés.

**2) La mise en œuvre des responsabilités pénales dans le cadre de l'exécution d'un contrat cloud**

***651.*** À l'instar de la responsabilité civile, la loi prévoit des actions pénales spécifiques au profit de la personne morale victime de la divulgation de ses données confidentielles contre l'auteur et éventuellement le complice. Il est question d'étudier, de manière distincte, les différentes actions pénales pouvant être exercées par le Client à l'encontre de son Prestataire et éventuellement de son sous-traitant.

***652. L'action pénale en contrefaçon.*** À la suite du développement de l'action civile en contrefaçon dans le développement précédent[1556], il est possible de sanctionner le délit de contrefaçon dans le cadre d'une procédure pénale. L'action pénale est « exclusivement celle du ministère public qui agit au nom de l'État pour faire réprimer une infraction pénale, c'est-à-dire un comportement interdit et passible de sanctions judiciaires les plus sévères, soit les peines pénales qui poursuivent un double but de dissuasion et de protection de l'ordre public »[1557]. Le Client, personne morale, peut se constituer partie civile à l'action du ministère public. Il est constaté qu'en matière du droit des marques « le ministère public n'engage pas d'action à sa propre initiative, *de facto*, les poursuites pénales pour contrefaçon n'étant diligentées que sur plainte avec constitution de partie civile »[1558]. En revanche, il existe une procédure de citation directe ouverte en matière de contrefaçon (en raison de l'absence de nécessité d'une instruction) permettant à la victime de saisir le tribunal correctionnel conformément aux articles 389 à 392-1 et 550 à 566 du code de procédure pénale. Dès lors le Client, personne morale, a la possibilité d'engager l'action à l'encontre de son Prestataire de services ; il faudra uniquement que la citation directe comporte « dans ses motifs un exposé détaillé des faits reprochés et viser le texte de loi qui les réprime »[1559].

***653.*** La particularité de l'action pénale, en contrefaçon par rapport à l'action civile, est l'exigence de démontrer un élément intentionnel en sus de l'élément matériel caractérisant la

[1556] V. *supra* n° 637 (action civile en contrefaçon).

[1557] Matsopoulou H. et Mascala C. (sous la direc.), 3087 – L'action pénale en contrefaçon en général, Le Lamy droit pénal des affaires, mis à jour 11/2021.

[1558] Binctin N., Marque – Droit pénal de la contrefaçon, Répertoire de droit commercial, Dalloz, Octobre 2020 (actualisation : mai 2022). Pour une illustration de l'appréciation de l'élément intentionnel, v. également, Crim. 4 avr. 2018, no 16-87.414.

[1559] Ibid.

contrefaçon[1560]. L'objectif d'engager une action pénale est de condamner l'auteur de l'atteinte à un droit de propriété intellectuelle et industrielle à des sanctions pénales telles qu'une peine d'emprisonnement et une amende. Concernant les sanctions pénales, le contrefacteur peut encourir, à titre principal, une peine de trois ans d'emprisonnement et de 300 000 euros d'amende[1561], et si le contrefacteur est lié par contrat avec la victime alors ces peines sont doublées[1562]. La complicité du contrefacteur d'un délit peut être reconnue en matière de contrefaçon[1563]. Il s'agirait ainsi de permettre d'inclure à la procédure le sous-traitant du Prestataire ou un tiers en cas de complicité avérée. Le juge pénal peut, également, prononcer des peines complémentaires afin de réparer l'intégralité des préjudices de la partie lésée « sans perte ni profit pour aucune des parties ». Pour cela, il est pris en compte « les conséquences économiques négatives, dont le manque à gagner, subi par la partie lésée, les bénéfices réalisés par le contrefacteur et le préjudice moral causé »[1564]. Par ailleurs, si le contrefacteur est une personne morale (ce qui est notre cas dans notre étude), l'article 121-2 du code pénal précise que la personne morale est responsable pénalement des infractions commises, pour leur compte, par leurs organes ou représentants et encourt une amende dans les conditions de l'article 131-38 du code pénal ainsi que les peines prévues à l'article 131-39 dudit code[1565]. En outre, la responsabilité pénale de la personne morale n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits en application de l'article 121-2 du code pénal. En l'espèce, le prestataire de services de cloud computing est très souvent une personne morale ; en conséquence, en cas de condamnation pénale, elle devra s'acquitter d'une amende. En revanche, il sera possible en sus d'engager la responsabilité pénale des personnes physiques en qualité d'auteur ou de complice ; ces derniers, en sus de la condamnation au paiement d'une amende, pourront être condamnés à une peine d'emprisonnement. Il en résulte que la loi pénale réprime sévèrement le délit de contrefaçon, ce qui devrait dissuader les prestataires de services cloud de commettre à, l'encontre de leurs clients, un délit de contrefaçon. La répression pénale, en matière de contrefaçon, permet de renforcer la protection du patrimoine informationnel numérique dans le cadre de l'exécution d'un contrat de cloud computing.

[1560] Ibid.

[1561] V. art. L.335-2-1's du CPI.

[1562] V. art. L.335-9 du CPI.

[1563] V. art. L.121-7 du C. pén.

[1564] Binctin N., Marque – Droit pénal de la contrefaçon, Répertoire de droit commercial, *op. cit.*.

[1565] Crim. 4 avr. 2018, pourvoi n° 16-87.414 et Crim. 26 juin 2019, pourvoi n° 17-87.485.

***654. L'action pénale fondée sur l'abus de confiance***. L'abus de confiance fait référence à « un comportement malhonnête consistant à trahir la confiance »[1566]. Il est un autre chef utilisé dans le cadre d'une action pénale et désigne « le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé »[1567]. La définition légale[1568] est assez large pour couvrir le détournement par le prestataire des données confidentielles de l'entreprise cliente hébergées dans le cloud. En effet, l'abus de confiance porte sur la remise d'une chose qui peut être « des fonds, des valeurs ou un bien quelconque ». L'abus de confiance peut, donc, concerner un bien corporel ou incorporel[1569], tel qu'une donnée numérique. Concernant l'auteur de l'abus de confiance, il est admis que la personne morale puisse être tenue pour responsable[1570] par le biais de ses dirigeants de droit effectifs [1571] ou des dirigeants de fait[1572]. Également, à l'instar du délit de contrefaçon, la complicité d'abus de confiance est punissable[1573]. Étant une infraction intentionnelle, il est nécessaire, au succès de cette action, d'apporter la preuve de l'élément intentionnel du détournement des biens. En l'espèce, il faudra apporter la preuve que le prestataire a abusé de la confiance de son client, personne morale, en détournant ses données. Ce délit se caractérise par la non-restitution ou l'usage abusif de la chose[1574]. L'abus de confiance peut être retenu à l'encontre du prestataire de services cloud lorsqu'il commet un usage abusif des données de son client. Cet usage abusif des données pourrait être constitué dès lors que le prestataire exploite les données de son client sans son consentement. En l'espèce, il peut s'agir d'un usage des données non conforme aux prévisions contractuelles dès lors qu'il est prévu une clause de non-exploitation des données ou lorsque le contrat cloud ne prévoit aucune clause relative à une licence d'exploitation des données. En réalité, ici, « ce qu'on lui reproche n'est pas tant d'avoir porté atteinte au patrimoine d'autrui que de s'être délié de ses engagements au préjudice d'autrui, c'est-à-dire d'avoir tiré profit d'une situation préalablement constituée, au mépris de ses obligations »[1575].

---

[1566] Matsopoulou H. et Mascala C. (sous la direc.), chap.5, Responsabilité pénale et sanctions, Le Lamy droit pénal des affaires, Mis à jour 11/2021.

[1567] V. art. 314-1 C. pén.

[1568] Ibid

[1569] Pour une illustration, v. Cass.crim 19 juin 2013, pourvoi n° 12-83.031.

[1570] V. *supra* n° 644 et suivants (les responsabilités pénales).

[1571] Cass. crim., 23 nov. 2016, nº 15-83.789.

[1572] Cass. crim., 25 févr. 2004, nº 03-80.759.

[1573] C. pén., art. 121-6 et 121-7. Pour une illustration, v. Cass. crim., 16 sept. 2014, nº 12-83.205.

[1574] Matsopoulou H. et Mascala C. (sous la direc.), chap.5, Responsabilité pénale et sanctions, Le Lamy droit pénal des affaires, mis à jour 11/2021.

[1575] Lajus-Thizon E., L'abus en droit pénal, Dalloz, Coll. NBT, 2011.

En général, dans le cadre d'une relation contractuelle (ce qui est notre cas ici), l'abus de confiance est le chef de poursuite le plus couramment utilisé.

***655.*** L'action pénale pour abus de confiance, comme envisagé ci-dessus[1576], est exercée par le ministère public après réception de la plainte de la victime de l'abus de confiance. Cette dernière devra se constituer partie civile si elle souhaite obtenir une réparation de son préjudice. Concernant les sanctions, l'abus de confiance fait encourir à titre principal, pour les personnes physiques, cinq ans d'emprisonnement et de 375 000 euros d'amende[1577] et pour les personnes morales une amende dans les conditions de l'article 131-38 du code pénal ainsi que les peines prévues à l'article 131-39 du code pénal[1578]. En revanche, il est précisé à l'article 121-2 du code pénal que « la responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits ». À ce titre, la responsabilité pénale des personnes physiques au sein de la personne morale pourra être recherchée dès lors qu'ils sont soit auteur soit complice du délit d'abus de confiance. En sus des peines prononcées à titre principal, le juge peut ordonner des peines complémentaires[1579]. Il en résulte qu'à l'instar du délit de contrefaçon, la loi pénale réprime sévèrement le délit d'abus de confiance, ce qui devrait aussi dissuader les prestataires de services cloud de commettre à, l'encontre de leurs clients, un délit d'abus de confiance. La répression pénale permet, ainsi, de renforcer la protection du patrimoine informationnel dans le cadre de l'exécution d'un contrat de cloud computing.

***656. L'admission d'un vol de données numériques.*** En l'espèce, il convient d'analyser la caractérisation du « vol » dans l'appropriation des données numériques. Dans un premier temps, le chef de poursuite utilisé dans le cadre de l'appropriation des données immatérielles se faisait par « le vol ». Dans un sens strictement juridique, l'article 311 du Code pénal dispose que le vol est « la soustraction frauduleuse du bien d'autrui ». Par cette définition, le bien est soustrait du patrimoine de la victime pour être transféré dans celui du « voleur ». Or, dans le cadre de la divulgation ou de l'appropriation des données immatérielles, l'information (bien immatériel) demeure dans le patrimoine de la victime. C'est pourquoi certains auteurs ont considéré que le vol ne peut porter que sur des biens matériels à l'exclusion de tout bien immatériel. Cependant, ces considérations n'ont pas empêché la Cour de cassation de développer une théorie du «vol d'énergie» dans son arrêt en date du 12 décembre 1984[1580] qui a permis à la Cour de cassation de retenir, dans son arrêt en date du 9 septembre 2003, la qualification de « vol de données

[1576] V. art.121-2 C. pén., et v. *supra* n° 647.

[1577] V. art. 314-1, al. 2 C. pén.

[1578] V. art. 314-12, al. 1er C. pén.

[1579] V. art. 314-10, 1° à 7° C. pén.

[1580] Cass.crim 12 décembre 1984, pourvoi n° 82-91.989, Bull.crim n°403.

informatiques ». Elle a considéré que : « le fait pour Emmanuel G. d'avoir en sa possession, à son domicile, après avoir démissionné de son emploi pour rejoindre une entreprise concurrente, le contenu informationnel d'une disquette support de logiciel Self Card, sans pouvoir justifier d'une autorisation de reproduction et d'usage du légitime propriétaire, qui au contraire soutient que ce programme source lui a été dérobé, caractérise suffisamment la soustraction frauduleuse de la chose d'autrui et la volonté de s'approprier les informations gravées sur le support matériel ; que le délit de vol est donc constitué à l'encontre d'Emmanuel G. » [1581]. En l'espèce, la Cour de cassation s'est rangée derrière une position plus au moins innovante de l'appréciation du chef de poursuite de « vol » en l'adaptant aux données informatiques. Cette décision a par la suite été confirmée dans plusieurs autres décisions juridictionnelles telles qu'un arrêt de la chambre criminelle de la Cour de cassation dans son arrêt en date du 4 mars 2008[1582]. Puis, dans le cadre d'un arrêt publié en date du 20 mai 2015[1583], la chambre criminelle a considéré que des données numériques constituent une chose susceptible d'être soustraite au sens de l'article 311-1 du Code pénal. En revanche s'agissant de la doctrine, celle-ci demeure divisée quant à l'utilisation du chef de poursuite de vol des biens immatériels et en particulier de données informatiques. À la question de savoir si la jurisprudence consacre le « vol d'information », Monsieur Saenko considère que « voir dans des données numériques une chose n'a rien d'hérétique puisqu'une donnée numérique n'est pas une information au sens strict ; elle n'est pas un savoir, une idée, une connaissance, mais une suite de chiffres intelligible qui, traduite par un programme informatique, permet la réalisation de certaines tâches »[1584]. Pour Monsieur Detraz, « les données numériques ne sont en outre pas totalement immatérielles »[1585]. Face à cette division doctrinale sur le « vol d'informations », une loi s'avérait nécessaire pour clarifier et apporter de la sécurité juridique quant à l'incrimination du « vol d'informations ». Depuis que la loi du 13 novembre 2014 [1586] a consacré à l'article 323-3 du Code pénal « l'extraction de données d'un système de traitement automatisé » est punie de cinq ans d'emprisonnement et

[1581] Cass. Crim 9 septembre 2003 n°02-87.098.

[1582] Cass.crim. 4 mars 2008 n°07-84.002, inédit.

[1583] Cass. Crim. 20 mai 2015, nº 14-81.336 : En l'espèce, il s'agissait d'un individu, qui avait eu fortuitement accès au système extranet de l'Agence nationale de sécurité sanitaire de l'alimentation, en avait profité pour télécharger des données numériques qu'il avait diffusées par la suite. Il ressort de la décision de rejet que, pour la Cour suprême, le téléchargement, effectué sans le consentement de leur propriétaire, de données que le prévenu savait protégées caractérise la soustraction frauduleuse constitutive du vol : Répertoire de droit pénal et de procédure pénale - Vol – Vol simple : ses composantes – Mihman A. ; Lucas De Leyssac M-P., – Avril 2016.

[1584] Saenko L., Vol par téléchargement de données numériques, D. 2015. 1466.

[1585] Detraz S., Vol de données informatiques, Gaz. Pal. 2015, no 169, p. 8.

[1586] La loi n°2014-1353 du 13 novembre 2014, consacre à l'article 323-3 du code pénal l'extraction de données d'un système de traitement automatisé.

d'une peine d'amende, [1587] le fait d'extraire les données d'un système de traitement automatisé, ainsi que de les reproduire et de les transmettre ». Cet article consacre « ce qui pouvait être appelé "vol de données". Il n'est donc plus nécessaire de recourir — en la dénaturant — à l'infraction de vol de l'article 311-1 du Code pénal »[1588]. Désormais, le « vol de données » ne relève plus du droit commun de l'article 311-1 du Code pénal[1589]. Il en résulte que dans le cadre de l'exécution d'un contrat de cloud computing, le Client, personne morale, pourra engager contre son Prestataire cette action pénale spécifique fondée sur l'article 323-3 du Code pénal dès lors que ce dernier aura procédé, sans le consentement de son client, à une extraction des données du cloud. Les sanctions, ici, sont dissuasives puisqu'elles portent sur une peine de cinq ans d'emprisonnement et d'une d'amende. Dans ce sens, la consécration du délit de « l'extraction de données d'un système de traitement automatisé » permet de renforcer la protection des données confidentielles des personnes morales en particulier lorsque celles-ci sont stockées dans l'informatique en nuage.

[1587] La loi n° 2015-912 du 24 juill. 2015 porte le montant de l'amende de 75 000 € à 150 000 €.

[1588] Répertoire de droit pénal et de procédure pénale, Vol – Vol simple : ses composantes – Mihman A. ; De Leyssac M-P-L. – Avril 2016.

[1589] Dreyer E., Consécration – provisoire du vol de données informatiques, AJ pénal 2015. 413.

# Conclusion du chapitre 1

***657. Le renforcement de la protection du patrimoine informationnel par le droit de la propriété intellectuelle et industrielle.*** Le renforcement de la protection du patrimoine informationnel réside dans l'application de régimes juridiques spécifiques en fonction du type de données concernés. La protection des données confidentielles de la personne morale peut être renforcée par le droit de la propriété intellectuelle et industrielle et en particulier par l'application, d'une part, du régime du secret applicable au savoir-faire et au secret de fabrique, et d'autre part, de droits spécifiques tels que le droit d'auteur et le droit sui generis du producteur de la base des données.

***658. Le renforcement de la protection du patrimoine informationnel par le droit commun des affaires.*** Le droit de la propriété intellectuelle et industrielle ne suffit pas à lui seul d'assurer la protection des données confidentielles des personnes morales, il a fallu adjoindre, le droit commun des affaires et en particulier le « secret des affaires ». La consécration du droit au secret des affaires a permis d'élargir le champ de la protection et les responsabilités délictuelles afin d'engager la responsabilité des acteurs et des complices qui sont à l'origine de l'atteinte au patrimoine informationnel.

***659. Une nécessaire prévision contractuelle***. Qu'il s'agisse du renforcement par le droit de la propriété intellectuelle et industrielle que du droit commun des affaires, il apparaît nécessaire, d'intégrer et d'adapter ces principes légaux dans le contrat de cloud computing par des dispositions particulières pour renforcer la protection du patrimoine informationnel de la personne morale. Cette étude a, donc, consister à élaborer des propositions rédactionnelles de clauses en faveur d'un renforcement de la protection des données dans le cadre de l'exécution d'un contrat de cloud computing.

# Chapitre 2 : Le renforcement de la protection des données par le contrat

***660. L'intégration des risques dans le champ contractuel.*** Lorsque la personne morale de droit privé conclut un contrat de cloud computing, elle consent à ce que son patrimoine informationnel soit hébergé dans une infrastructure cloud. Ce patrimoine informationnel a plus de valeur que les services rendus dans le cadre du contrat de cloud computing en raison qu'il est composé des actifs immatériels de l'entreprise. La personne morale doit, donc, s'assurer que le contrat de cloud computing prévoit des garanties efficaces en matière de protection de ses données composant le patrimoine informationnel. Afin de proposer des prévisions contractuelles, il convient d'identifier, en amont, les risques pesant sur la protection des données.

***661. La mise en place de garanties conventionnelles efficaces.*** Les garanties pouvant être déployées afin de renforcer la protection du patrimoine informationnel peuvent être de deux sortes ; il s'agirait d'une part, de prévoir une sécurisation conventionnelle consistant à intégrer dans le champ contractuel les risques en matière d'obligations juridiques et d'autre part, de concevoir la sécurisation conventionnelle par une alliance de la technologie au contrat.

***662. Plan.*** Il est proposé d'étudier le renforcement de la protection des données par la sécurisation conventionnelle en intégrant, d'une part, les obligations juridiques (**Section 1**) et d'autre part les garanties techniques (**Section 2**).

## Section 1 : Le renforcement de la protection des données par la sécurisation conventionnelle en matière d'obligations

***663.*** Afin de renforcer la protection des données de la personne morale, il est proposé de sécuriser juridiquement certaines dispositions du contrat de cloud computing. En particulier, notre attention est portée, ici, sur les clauses qui ont trait aux obligations du prestataire et à la responsabilité contractuelle.

***664.*** **Plan.** Il est envisagé d'étudier le renforcement de la protection des données de la personne morale par l'encadrement conventionnel des obligations du prestataire (A) et de la responsabilité du prestataire (B).

## A) Le renforcement de la protection par l'encadrement conventionnel des obligations du prestataire

***665.*** ***Une sécurité juridique***. Cette partie a pour objet d'étudier les clauses dans le contrat de cloud computing relatives à la sécurité juridique, c'est-à-dire celles qui permettent de prémunir le client d'un risque juridique quant à une éventuelle atteinte de ses droits à la protection des données. En particulier, il s'agit d'intégrer dans le contrat des clauses qui vont imposer certaines obligations au prestataire afin de renforcer la protection des données de la personne morale.

***666.*** ***Plan.*** En l'espèce, il est envisagé d'analyser les clauses relatives aux obligations de confidentialité (1), de faire et de ne pas faire (2).

### 1) L'intégration conventionnelle d'une obligation de confidentialité

a) La détermination du contenu de la clause de confidentialité des données

***667.*** ***La confidentialité des données versus le secret du dépôt.*** La question de la préservation de la confidentialité des données est centrale dans le contrat de cloud computing en raison du caractère secret attaché à certaines données et doit, donc, pouvoir être garantie efficacement. L'obligation de confidentialité des données fait écho au secret du dépôt prévu à l'article 1931 du Code civil qui impose au dépositaire qu'« il ne doive pas chercher à connaître quelles sont les choses qui lui ont été déposées, si elles lui ont été confiées dans un coffre fermé ou sous une enveloppe cachetée »[1590]. Si nous transposons ce texte au contrat de cloud computing, il s'agirait de considérer que le prestataire de services cloud ne doit pas connaître le contenu des données de son Client hébergées dans son infrastructure cloud. Il en résulterait, donc, une interdiction d'accès et d'exploitation des données à la charge du Prestataire. Bien qu'il s'agisse d'un texte ancien non revisité depuis 1804, il permet de prendre la mesure de ce qui est attendu par le client sur le plan de la confidentialité de ses données.

***668.*** ***La confidentialité, une clause fondamentale pour la protection des données.*** Il est rappelé, ici, que la confidentialité des données, au même titre que la disponibilité[1591] et l'intégrité[1592] des données sont fondamentales pour assurer la sécurisation des données hébergées dans le cloud. La confidentialité est protégée « par différentes réglementations spécifiques, telles que la

[1590] Article 1931 du code civil, relative au secret du dépôt (rédaction en vigueur depuis 1804).

[1591] V. *infra* n° 715 et suivants.

[1592] Ibid.

protection de la propriété intellectuelle ou des données, leur sort dans le cadre des contrats infonuagiques relève de dispositions négociées »[1593]. Ainsi, en amont de la signature d'un contrat cloud, le client, personne morale, devra s'assurer que celui-ci intègre une clause de confidentialité pour protéger le patrimoine informationnel de l'entreprise. À ce titre, le Professeur Jean-Marc Mousseron indique, concernant la protection des données par l'engagement de confidentialité, que « l'utilisation de mécanismes contractuels peut s'avérer indispensable, par exemple lorsque dans le contexte d'une négociation avec un tiers, l'accès doit être accordé à une partie du savoir-faire. Le titulaire devra imposer au tiers la signature d'un accord de confidentialité. Ce type d'accord se divise le plus souvent en deux obligations : une obligation de non-divulgation à des tiers du savoir-faire, et une obligation de non-exploitation de ce savoir-faire »[1594]. Ainsi, pour renforcer la protection des données dans les contrats de cloud computing, il est recommandé que le contrat puisse prévoir un engagement de confidentialité des données du client, lesquelles sont sensibles et ont trait à la stratégie des entreprises.

***669. L'identification de la confidentialité***. Cette clause a pour objet de mettre à la charge du prestataire de services cloud une obligation de confidentialité des informations de son client, lesquelles ont été identifiées et désignées comme étant confidentielles dans le cadre du contrat[1595]. Dès lors qu'une information sera identifiée et désignée comme confidentielle, le prestataire de services cloud s'engage à ne pas la divulguer à un tiers et à se conformer aux dispositions du contrat et de la loi[1596].

[1593] Bourgeois M., JurisClasseur Communication, Fasc. 962 : CLOUD COMPUTING – Les défis contractuels du Cloud Computing, 1er mai 2020. Egalement, v. *supra* n° 569 et suivants.

[1594] Mousseron J-M, Secret et contrats – de la fin de l'un à la fin de l'autre –, Mélanges Foyer, 1997, PUF, p. 257.

[1595] Illustration du champ des « données confidentielles » dans le contrat de solutions Cloud de la société Dell : « Le terme « Informations confidentielles » désigne (i) les données que le Client transmet ou conserve dans la Solution ou les informations fournies à Dell par le biais d'un Formulaire de commande ; (ii) la tarification et les autres documents Dell s'appliquant à la Solution, les Instructions d'activation, les informations relatives au marketing et aux ventes , le savoir-faire, les rapports d'audit et de sécurité, les plans de développement de produits, les conceptions de data center (y compris les informations non graphiques que le Client peut observer lors d'une visite d'un data center, ou toute autre information ou technologie fournie par Dell [y compris un Logiciel]) ; et (iii) les Secrets commerciaux ou toute information indiquée comme étant de nature confidentielle. Les informations développées sans qu'aucune référence aux Informations confidentielles de l'autre partie ou qui relèvent du domaine public ou tombent dans le domaine public, ou bien qui sont mises à disposition de l'autre partie sans violation des obligations de confidentialité, ne constitueront pas des Informations confidentielles ».

[1596] V. *supra* n° 567 et suivants relatifs à la protection des données des personnes morales par la loi.

b) L'encadrement conventionnel de l'obligation de confidentialité du Prestataire

***670. Le renforcement de la protection des données par une clause de confidentialité***. Il s'agirait, ici, d'élargir conventionnellement l'obligation de confidentialité à l'ensemble des données et non uniquement à certains types de données protégées par un droit privatif[1597] ou un secret spécifique (savoir-faire, secret de fabrication)[1598]. Pour une raison d'efficacité, cette clause relative à la confidentialité doit prévoir les sanctions en cas de contravention à cette obligation, telles que l'engagement de la responsabilité civile et éventuellement pénale du prestataire, la résiliation du contrat cloud à la charge du prestataire et le paiement d'une indemnité au profit du client. Il est proposé d'intégrer cette clause sous la section relative aux obligations du prestataire et de l'intituler « Obligations du Prestataire relatives à la confidentialité des données du client ». Il est présenté, ci-après, une proposition de rédaction de clause de confidentialité :

***671.*** « Le Prestataire s'engage à ne communiquer les données confidentielles appartenant au client à aucune personne ou entité et à prendre toutes mesures nécessaires pour éviter que son personnel ne divulgue à des tiers tout ou partie desdites données. Le Prestataire s'engage à ne pas entreprendre d'actions directes ou indirectes susceptibles de mettre en péril la confidentialité des données stockées dans le cloud. Également, le Prestataire s'engage à garantir la confidentialité des données du client en mettant en œuvre tous les moyens techniques nécessaires pour sécuriser le cloud contre toute ingérence ou intrusion de tiers non autorisés. En cas de contravention, aux présentes dispositions, le Prestataire engage sa responsabilité avec pour sanction le paiement au profit du Client d'une indemnisation compensatrice d'un montant équivalent à X % du montant du préjudice évalué. Étant précisé qu'en cas de désaccord sur l'évaluation du montant du préjudice, il sera possible pour l'une ou l'autre des parties au contrat de faire appel à une expertise. En cas de contravention par le Prestataire à l'une des obligations du présent article, le Client dispose, également, de la faculté de résilier le présent contrat à la charge du Prestataire ».

***672. Le renforcement de la protection des données par un accord de confidentialité.*** Il est, également, possible de prévoir, au lieu de l'insertion dans le contrat de cloud computing d'une clause de confidentialité, un accord de confidentialité qui figurera en annexe du contrat cloud. Ce type d'accord peut être mis en parallèle avec la proposition rédactionnelle, ci-dessus, d'un

[1597] V. *supra* n° 569 et suivants relatifs à la protection par la propriété intellectuelle ou industrielle.

[1598] V. *supra* n° 579 et suivants relatifs à la protection par le savoir-faire et secret de fabrication.

accord de protection des données de secret d'affaires[1599]. Cet accord de confidentialité a un champ plus large que l'accord de protection des données de secret d'affaires, car il concerne tous types de données de la personne morale et non uniquement celles qui renferment le secret des affaires. En conséquence, la protection par un accord de confidentialité est plus étendue. Concernant le contenu de l'accord de confidentialité, il est préconisé d'intégrer un certain nombre d'éléments; lesquels sont les suivants : « une reconnaissance de principe du caractère entièrement confidentiel de toutes les données stockées et de toutes les opérations et traitement réalisés par le client sur et par le truchement des serveurs et de l'infrastructure du prestataire ; en conséquence, l'interdiction au prestataire de prendre connaissance du contenu de ces données ou de ces opérations de traitements, au-delà de ce qui leur est absolument nécessaire pour pouvoir assurer leurs prestations ; l'engagement du prestataire de faire respecter cet engagement par tous ses salariés ou commettants et de communiquer à des tiers non autorisés ou de les laisser accéder à ces données et informations confidentielles du client ; l'engagement du prestataire de mettre en œuvre des moyens de sécurité (à définir en annexe technique) pour assurer la sécurité et la confidentialité des données et informations dont le client a confié la garde et l'hébergement au prestataire ; l'obligation imposée au prestataire de prévenir le client de tout incident ayant mis en cause la confidentialité de ses données ou traitements »[1600]. En prenant en considération les éléments énoncés ci-dessus, il est présenté, ci-après, un modèle d'accord de confidentialité en matière de protection des données dans le cadre d'une opération contractuelle de cloud computing :

**ACCORD DE CONFIDENTIALITÉ DES DONNÉES HÉBERGÉES DANS LE CLOUD**

**ANNEXE AU CONTRAT DE CLOUD COMPUTING**

entre

**.....,** société ..... *(forme de la société)*, ayant son siège social ..... *(adresse du siège social)*, enregistrée au Registre du Commerce et des Sociétés de ..... *(localité du RCS),* sous le numéro ..... *(n° RCS)*, représentée par M. / Mme..... (nom du représentant), ..... *(qualité du représentant),* dûment habilité à l'effet des présentes,

ci-après désigné(e) par **« le Prestataire »,**

**D'UNE PART,**

[1599] V. *supra* n° 630, proposition rédactionnelle d'un accord de secret.

[1600] Warusfel B. (sous la direction de Vivant M.), Le Lamy droit du numérique 2018, Expert, Partie 3 - Numérique et contrats, division 3 - Les principaux contrats du numérique et leurs spécificités, chapitre 6 - Les contrats d'informatique dématérialisée (cloud computing), p.493 n°710, mis à jour 22 avril 2022.

**ET**

**.....,** société ..... *(forme de la société)*, ayant son siège social ..... *(adresse du siège social)*, enregistrée au Registre du Commerce et des Sociétés de ..... *(localité du RCS),* sous le numéro ..... *(n° RCS)*, représentée par M. / Mme ..... (nom du représentant), ..... *(qualité du représentant),* dûment habilité à l'effet des présentes,

ci-après désigné(e) par **« le Client »,**

**D'AUTRE PART,**

**PRÉAMBULE**

Dans le cadre de la conclusion d'un contrat de cloud computing, les Parties acceptent d'annexer au contrat de cloud computing (ci-après désigné contrat principal), le présent accord relatif à la confidentialité des données hébergées dans l'infrastructure en nuage.

Afin de protéger l'ensemble des informations confidentielles du Client hébergées dans l'infrastructure en nuage du Prestataire, les Parties ont l'intention de s'engager juridiquement et sont convenues de ce qui suit :

**Article 1 - Définitions**

**1.1 1.1** Le terme « DONNÉES CONFIDENTIELLES », désigne les informations de toute nature détenues par le Client incluant de manière non limitative : le savoir -faire, le secret de fabrique, les informations de nature commerciale (étude de marché, portefeuille client et fournisseur de l'entreprise…), financière (informations sur le chiffre d'affaires, bénéfices, pertes ), contractuelle (conditions particulières accordées telles que les prix, ristournes, quantités achetées, date d'expiration de garanties...), marketing (stratégies de communication et de développement, procédés et outils marketing utilisés), technique (procédés techniques de développement des produits, logiciel, code-source..) et plus généralement, toute documentation sous format électronique s'y rapportant. En particulier, sont confidentielles les informations ayant une valeur économique réelle ou potentielle ou un avantage concurrentiel certain propre dont le public ou toute autre personne, y compris le Prestataire, pourrait retirer de leur divulgation ou utilisation une valeur économique ou un avantage concurrentiel.

Ces DONNÉES CONFIDENTIELLES constituent l'objet du présent accord et seront avec le présent Engagement tenus pour confidentiels.

**Article 2 – Objet**

L'accord a pour objet de fixer les règles relatives à la protection des DONNÉES CONFIDENTIELLES appartenant exclusivement au Client et qui sont hébergées dans l'infrastructure en nuage du Prestataire.

Le présent accord couvre, également, l'ensemble des discussions relatives au contrat principal et la période de discussion, de négociation et d'exécution dudit contrat.

**Article 3 – Déclarations du Client**

Le Client déclare qu'il bénéficie d'un droit de propriété exclusif sur ses DONNÉES CONFIDENTIELLES et n'accorder, au Prestataire, aucun droit sur lesdites données.

**Article 4 - Obligations du Prestataire**

**4.1** Le prestataire s'engage à garantir la confidentialité des DONNÉES CONFIDENTIELLES du client en mettant en œuvre tous les moyens techniques nécessaires pour sécuriser le cloud contre toute ingérence ou intrusion de tiers non autorisés.

**4.2** Le Prestataire s'engage à ne communiquer les DONNÉES CONFIDENTIELLES appartenant au Client à aucune personne ou entité et à prendre toutes mesures nécessaires pour éviter que son personnel ne divulgue à des tiers tout ou partie desdites données.

**4.3** Le Prestataire s'engage à ne pas entreprendre d'actions directes ou indirectes susceptibles de mettre en péril la confidentialité des données hébergées dans le cloud, objet du contrat, sous peine de voir sa responsabilité engagée conformément à l'article 7 du présent accord.

**4.4** Le Prestataire s'engage à ne pas accéder, à utiliser, traiter, exploiter les DONNÉES CONFIDENTIELLES sans une autorisation préalable du Client.

**4.5** Le Prestataire s'engage à ne pas troubler la jouissance paisible du droit de propriété du Client sur ses DONNÉES CONFIDENTIELLES et s'interdit de réaliser une quelconque action ou manipulation technique sur lesdites données de son Client, entendu largement et de manière non limitative comme : toute utilisation, toute duplication, tout traitement, toute exploitation, toute représentation, toute reproduction et toute transmission.

**4.6** S'agissant de l'utilisation de certaines données prévue à l'article 6 du présent accord, le Prestataire s'engage à ne procéder à aucune duplication, sous quelque forme et quelque support que ce soit, de tout ou partie de l'information transmise, sans l'autorisation écrite et préalable du Client.

**4.7** Dans les trente (30) jours suivant l'expiration du contrat de cloud computing, le Prestataire s'engage à restituer ou à détruire l'intégralité des DONNÉES CONFIDENTIELLES en sa possession et certifier par écrit ne pas avoir conservé de DONNÉES CONFIDENTIELLES et/ou de reproductions, sur quelque support que ce soit.

**Article 5 – Propriété des données**

**5.1** Le Client demeure le propriétaire exclusif de ses DONNÉES CONFIDENTIELLES qui sont hébergées dans les serveurs de l'infrastructure en nuage du Prestataire.

**5.2** Le présent Accord n'autorise aucun transfert de propriété sur ses DONNÉES CONFIDENTIELLES au profit du Prestataire.

**5.3** Le présent Accord ne peut, en aucun cas, être interprété comme conférant de manière implicite une concession de licence de brevet, de marque ou d'autres droits de propriété intellectuelle ou industrielle reconnus par la loi.

**Article 6 – Utilisation autorisée de certaines DONNÉES CONFIDENTIELLES**

Le Prestataire ayant connaissance d'une DONNÉE CONFIDENTIELLE s'engage à ne l'utiliser que dans le cadre du présent Contrat et pour les seuls besoins pour lesquels cette information est communiquée et reconnaît que cette information reste, en tout état de cause, la propriété du Client.

**Article 7 - Responsabilité et clause pénale**

En cas de contravention à l'une des dispositions du présent Accord et plus généralement d'une atteinte à la protection des DONNÉES CONFIDENTIELLES, le Prestataire s'engage à réparer l'intégralité des préjudices qui résulteront de cette atteinte sans opposer une quelconque limitation de responsabilité dès lors que l'atteinte est avérée et lui est imputable. À ce titre, le Prestataire s'engage à verser au profit du Client une indemnisation compensatrice d'un montant équivalent à X % du montant du préjudice évalué. En cas de désaccord sur l'évaluation du montant du préjudice, il est possible pour l'une ou l'autre des parties de faire appel à une expertise conformément à l'article 10 du présent accord.

**Article 8 – Durée**

L'Accord entre en vigueur à compter de la date de signature du contrat principal par les Parties et est conclu pour la durée de validité du contrat principal.

**Article 9 – Résiliation**

L'accord ne peut être résilié indépendamment de la résiliation du contrat principal signé entre les Parties.

**Article 10 – Litiges et droit applicable.**

**9.1** Le présent accord est soumis à la réglementation française en vigueur.

**9.2** En cas de contestation, les Parties peuvent décider, individuellement ou collectivement, de mandater un expert aux fins de constatations, de délimitation du champ de l'atteinte aux droits du Client sur ses DONNÉES CONFIDENTIELLES et de détermination de l'étendue du préjudice réparable.

**9.3** En cas de désaccord, les Parties s'engagent, en priorité, à privilégier la résolution du litige à l'amiable avant tout recours contentieux.

**9.4** En cas de contestation persistante, les Parties acceptent de soumettre leur différend aux juridictions françaises compétentes.

Fait le ..... *(date),* A ..... *(lieu),*

En deux exemplaires originaux,

Pour le Prestataire (signature)

Pour le Client (signature)

***673.*** Toujours dans un objectif de renforcement de la protection des données de la personne morale, il est préconisé, en sus de l'engagement de confidentialité, d'adjoindre dans le contrat de cloud computing, des clauses relatives à une obligation d'information et de mise en garde du prestataire ainsi qu'une interdiction générale d'exploitation des données par le Prestataire lesquelles sont étudiées dans la partie suivante.

**2) L'intégration conventionnelle d'une obligation de faire et de ne pas faire**

***674.*** Afin de renforcer la protection des données confidentielles de la personne morale, il est proposé de parfaire la sécurisation contractuelle en intégrant dans le contrat des dispositions relatives à des obligations de faire et de ne pas faire. L'obligation de faire consisterait à mettre à la charge du prestataire une obligation d'information et de mise en garde. Quant à l'obligation de ne pas faire, il s'agirait de prévoir une obligation de ne pas exploiter les données confidentielles de la personne morale.

***675.*** Il est envisagé, d'une part, d'étudier l'intégration d'une clause relative au droit d'information et de mise en garde au profit du client (a) ainsi qu'une clause relative à l'interdiction de l'exploitation des données (b).

a) L'intégration conventionnelle d'une obligation d'information

***676.*** Outre l'obligation générale de bonne foi[1601] et d'obligation générale d'information précontractuelle[1602] applicables à tous les contrats, il n'existe pas à l'heure actuelle une disposition légale consacrant une obligation d'information à la charge du prestataire de services de cloud computing et au profit des personnes morales. Il s'agit d'une lacune légale qui est susceptible d'être compensée par l'ingénierie contractuelle. En l'occurrence, il s'agirait de prévoir dans le contrat cloud une clause ayant pour objet de mettre à la charge du prestataire de services cloud une obligation générale de « conseil, d'information et de mise en garde »[1603]. À ce titre, il est présenté, ci-après, une proposition de rédaction de clause relative à cette obligation générale de « conseil, d'information et de mise en garde » applicable dans le cadre d'un contrat de cloud computing :

***677.*** « Le Prestataire, préalablement à la conclusion du contrat, s'engage à communiquer au Client toutes les informations utiles et pertinentes concernant la prestation de services choisie par le Client. Il s'engage à remettre au client, avant la conclusion du contrat, la documentation

[1601] V. art.1104 C. civ. concernant le principe général de bonne foi applicable à tous les contrats.

[1602] V. art.1112-1 C. civ. concernant l'obligation générale d'information applicable à tous les contrats.

[1603] Warusfel B. (sous la direction de Vivant M.), Le Lamy droit du numérique 2018, Expert, Partie 3 - Numérique et contrats, division 3 - Les principaux contrats du numérique et leurs spécificités, chapitre 6 - Les contrats d'informatique dématérialisée (cloud computing), p.493 n°710, mis à jour 22 avril 2022.

technique et précontractuelle attachée à ladite prestation de services et à rester à la disposition du Client pour répondre aux éventuelles interrogations. Le Prestataire met en garde le Client de s'entourer de tous les conseils nécessaires à la contractualisation d'une offre de services cloud et en particulier concernant le choix des modules de services cloud. Le Prestataire informe le Client qu'il lui incombe de s'assurer de la pertinence et de l'adaptation de la prestation de services choisie par rapport à ses besoins et ses attentes. Le Prestataire informe le Client qu'il ne pourra pas être tenu pour responsable en cas d'erreur par le Client concernant le choix de la prestation de services ou leurs adaptations par rapport à ses besoins ».

***678.*** Il s'agit, donc, d'une proposition de clause dont l'objet est de mettre en garde le client concernant la pertinence de ses choix de services cloud afin de renforcer la protection des données, laquelle pourra être alimentée en fonction des besoins des parties et de l'opération cloud concernée. En outre, il apparaît opportun d'ajouter à cette clause d'information générale et de mise en garde, une clause relative au droit d'information du client concernant la localisation des données dont une proposition est présentée ci-après :

« Le Prestataire informe le Client que ses données sont hébergées dans des serveurs appartenant au Prestataire lesquels sont situés sur le territoire de l'Union européenne. Le prestataire s'engage à se conformer à la localisation des données choisie par le client lors de la souscription aux services cloud. Sauf accord contraire des Parties, le prestataire s'engage à ne transférer ni héberger aucune des données du Client dans des serveurs situés hors de l'Union européenne. Le Prestataire s'engage à informer, sans délai, le client lorsque les données sont transférées, pour un motif légitime (notamment en application d'une réglementation impérative ou une décision juridictionnelle ayant force obligatoire), dans un centre de données situé en dehors de la localisation choisie par le client ».

C'est par l'ingénierie contractuelle que le client peut recouvrir dans une certaine mesure, le contrôle sur ses données, du moins quant au choix de la localisation de ses données.

***679.*** Par l'intégration de ces clauses d'information et de mise en garde, le Client, personne morale, est titulaire conventionnellement d'un droit à l'information qui contribue au renforcement de la protection de ses données. En effet, le bénéfice de ce droit d'information permet au Client de gérer et contrôler ses données dans le cloud. En outre, pour conforter ce droit à l'information, le Client peut s'appuyer, également, sur des décisions juridictionnelles qui ont statué sur la question du droit à l'information du client et de l'obligation de mise en garde du prestataire de services. Dans des décisions, il a été jugé que « le prestataire de service à l'obligation d'informer son client, et même de le conseiller, en lui communiquant toute donnée

qui pourrait lui être utile »[1604]. Cette position jurisprudentielle permet de conforter le droit d'information des clients et ainsi renforcer par la même occasion la protection des données. C'est parce que le client sera mieux informé qu'il pourra prendre des décisions ou des actions en faveur d'un renforcement de la protection de ses données dans le cloud.

***680.*** Outre les clauses relatives à l'information du Client, il conviendrait de prévoir, également, dans le contrat de cloud computing, une clause relative à l'interdiction de l'exploitation des données des personnes morales.

b) L'intégration conventionnelle d'une obligation générale de non-exploitation des données

***681. La nécessité d'une interdiction conventionnelle d'exploitation des données.*** En principe un contrat de cloud computing ne doit pas autoriser le prestataire à traiter et à exploiter les données de son client en raison, notamment, de la particularité du contrat de cloud computing dont l'objet est de « mettre à la disposition, par le prestataire au profit du client, un espace de stockage pour y accueillir, selon le cas, soit des données (à des fins d'archivage par exemple), soit des données accompagnées d'une ou plusieurs application(s) logicielle(s), permettant leur traitement (généralement aux fins de réalisation d'une ou plusieurs tâche(s) métier) »[1605]. Il est, ainsi, primordial que la question du sort des données soit clairement précisée dans le contrat. Lorsque le Client contractualise une offre de services cloud, il doit s'assurer que le contrat mentionne, dans une disposition expresse, que les données confidentielles hébergées dans l'infrastructure en nuage du prestataire appartiennent au client. Cette indication permettra, ainsi, de préserver la protection de ses données. Pour renforcer l'effet protecteur de cette mention, il est nécessaire de prévoir une clause imposant au prestataire une obligation de ne pas exploiter les données de son client, personne morale.

***682. Le contenu protecteur d'une clause interdisant l'exploitation des données***. Dans la section des obligations incombant au prestataire de services cloud, il est préconisé, ainsi, de prévoir une clause prohibant l'exploitation des données stockées dans le cloud sous peine de mettre en péril la continuité du contrat cloud et l'allocation, au profit du client, d'une indemnisation correspondant à un certain montant lequel peut être envisagé de manière forfaitaire ou par l'établissement d'un pourcentage en fonction de la réalisation du chiffre d'affaires. En effet, il apparaît, ici, difficile de procéder à une estimation chiffrée de l'indemnisation permettant de

[1604] Civ. 1re, 11 juin 1996, pourvoi n°94-18.250. Bull. civ. I, n°245.

[1605] Bourgeois M., JurisClasseur Communication, Fasc. 962 : Cloud computing – Les défis contractuels du Cloud Computing, 1er mai 2020.

couvrir l'intégralité du préjudice subi par le client, personne morale. Il convient, donc, de s'interroger sur la méthode à retenir afin d'évaluer le montant de l'indemnisation permettant de réparer l'atteinte aux droits des clients sur leurs données. Pour une raison d'efficacité de la clause, la sanction financière doit correspondre à un montant très important afin de dissuader le prestataire de services de porter atteinte à la protection des données confidentielles. C'est la raison pour laquelle il est préconisé d'établir la sanction en se basant sur un pourcentage du montant du préjudice évalué.

***683. Une proposition d'un modèle de clause interdisant l'exploitation des données du client***. À titre de rédaction de clause, il est proposé d'intituler la clause « Obligation de non-exploitation des données du client » et dont une proposition est présentée, ci-après :

« Dans le cadre des présentes, le Client n'accorde au profit du Prestataire aucune licence d'exploitation de ses données lesquelles sont hébergées dans l'infrastructure en nuage du Prestataire. Les données sont entendues, ici, largement comme étant les informations de toute nature détenues par le Client incluant de manière non limitative : le savoir -faire, le secret de fabrique, les informations de nature commerciale (étude de marché, portefeuille client et fournisseur de l'entreprise…), financière (informations sur le chiffre d'affaires, bénéfices, pertes ), contractuelle (conditions particulières accordées telles que les prix, ristournes, quantités achetées, date d'expiration de garanties...), marketing (stratégies de communication et de développement, procédés et outils marketing utilisés), technique (procédés techniques de développement des produits, logiciel, code-source..) et plus généralement, toute documentation sous format électronique s'y rapportant. Le Client bénéficie d'un droit de propriété exclusif sur les données hébergées dans l'infrastructure du nuage du Prestataire. Le Prestataire s'engage à ne pas utiliser, traiter, exploiter les données hébergées dans l'infrastructure cloud sans le consentement préalable du Client. Également, le Prestataire s'interdit de réaliser une quelconque action ou manipulation technique sur lesdites données, entendu largement et de manière non limitative comme : toute utilisation, toute duplication, tout traitement, toute exploitation, toute représentation, toute reproduction et toute transmission.

En cas de contravention à la présente disposition, le Prestataire s'engage à réparer l'intégralité des préjudices qui résulteront de cette atteinte sans opposer une quelconque limitation de responsabilité dès lors que l'atteinte est avérée et lui est imputable. Le Prestataire sera redevable au profit du Client du paiement d'une indemnisation compensatrice d'un montant équivalent à xx % du montant du préjudice évalué. Le Client disposera de la faculté de résilier le contrat de cloud computing aux torts exclusifs du Prestataire.

En cas de contestation, les Parties peuvent décider, individuellement ou collectivement, de mandater un expert aux fins de constatations, de délimitation du champ de l'atteinte aux droits du Client sur ses œuvres et de déterminer l'étendue du préjudice réparable. En cas de désaccord, les Parties s'engagent, en priorité, à privilégier la résolution du litige à l'amiable avant tout recours contentieux. ».

***684.*** Malgré cette interdiction conventionnelle d'exploitation des données, le Prestataire peut l'enfreindre et conclure avec une autre entité « une convention de cession des données ». La contravention à cette obligation conventionnelle consisterait à transférer massivement un nombre important de données qui appartiennent à leurs clients contre l'obtention d'un avantage, telles qu'une rémunération ou la délivrance d'un service. Malgré l'interdiction conventionnelle, la cession va pouvoir produire ses effets et mettre ainsi en périls les données des personnes morales stockées dans le cloud[1606]. En revanche, dès lors que le manquement est constaté, le Client a la possibilité d'engager la responsabilité contractuelle et l'exécution de la clause pénale prévue au contrat.

***685.*** L'intérêt d'intégrer dans le contrat de cloud computing une clause interdisant l'exploitation est d'une part, de souligner les obligations à la charge du prestataire et d'autre part, de dissuader le prestataire à porter une atteinte au patrimoine informationnel de l'entreprise. Cette sécurisation contractuelle, par l'intégration d'une clause interdisant l'exploitation des données, permet de réduire les atteintes pouvant être portées aux données et ainsi renforcer la protection de celles-ci.

***686.*** Après avoir envisagé les prévisions contractuelles concernant les obligations à la charge du Prestataire, il est envisagé d'étudier celles qui ont trait à la responsabilité contractuelle du prestataire dans un contexte international.

## B) Le renforcement de la protection par l'encadrement conventionnel de la responsabilité contractuelle

***687. La sécurisation contractuelle des données de la personne morale***. Le client achète, en l'espèce, une prestation de services d'hébergement de données et doit, alors, pouvoir bénéficier de la sécurité de ses données. Par principe, le contrat de cloud computing doit prévoir, à titre d'obligation principale, que le prestataire s'engage à sécuriser son infrastructure en nuage. Pour renforcer la protection des données hébergées dans le cloud, il est nécessaire de prévoir des

[1606] Illustration avec l'affaire Cambridge analytica concernant la fuite de données de 87 millions d'utilisateurs de Facebook.

dispositions qui encadrent les obligations des parties au contrat, en particulier celles incombant au prestataire. L'intérêt est de pouvoir engager la responsabilité du prestataire en cas de manquement à une obligation conventionnelle. Il est, alors, envisagé d'étudier dans cette partie, les clauses relatives à la sécurité juridique, et plus particulièrement cette fois-ci, aux clauses qui ont trait à la responsabilité contractuelle du prestataire dans un contexte international.

***688.*** **Plan.** Cette partie a pour objet d'étudier le renforcement de la protection des données par les prévisions du contrat relatives à la responsabilité contractuelle (1) avec la prise en compte de l'extraterritorialité pour l'exécution du contrat de cloud computing (2)

**1) Le renfort des prévisions contractuelles en matière de responsabilité**

***689.*** ***La distinction d'obligation de moyens et de résultats.*** Bien que le contrat cloud puisse prévoir le périmètre dévolu à chacune des parties au contrat, il apparaît en pratique que des violations sont réalisées directement ou indirectement par les prestataires de services cloud. En présence d'un manquement aux obligations contractuelles du contrat de cloud computing[1607], le client, personne morale, peut engager une action en responsabilité contractuelle sur le fondement des articles 1103, 1193 et 1194 du Code civil contre son prestataire de services de cloud computing. La responsabilité du prestataire de services de cloud computing est une responsabilité de droit commun reposant sur la qualification d'obligations de moyens et de résultats. Dans ce sens, « l'obligation sera de moyen lorsqu'il sera question de la disponibilité du service alors qu'elle sera de résultat s'agissant de la récupération des données hébergées. En ce cas, seul un cas de force majeure pourra exonérer le prestataire de sa responsabilité »[1608] et sous réserve de l'aménagement du contrat par des clauses limitatives de responsabilité. Cette action en responsabilité contractuelle peut être fondée sur un manquement d'un engagement contractuel qui peut être contenu soit directement dans le contrat de cloud computing (clause de confidentialité, de non-concurrence)[1609] ou bien figurer dans un acte annexé au contrat de cloud computing (un accord de confidentialité)[1610].

[1607] V. *supra* n° 670, 671, 676 relatifs à des propositions rédactionnelles de clauses qui prévoient des obligations à la charge du prestataire (obligation d'information, de mise en garde, de non-exploitation des données).

[1608] Warusfel B. (sous la direction de Vivant M.), Le Lamy droit du numérique 2018, Expert, Partie 3 - Numérique et contrats, division 3 - Les principaux contrats du numérique et leurs spécificités, chapitre 6 - Les contrats d'informatique dématérialisée (cloud computing), p.491 n°704, mis à jour 22 avril 2022.

[1609] V. *supra* n° 664 relatif à la proposition rédaction d'une clause de confidentialité

[1610] V. *supra* n° 665 relatif à la proposition rédaction d'un accord de confidentialité.

***690. Le renforcement du droit à réparation conventionnel dans le cadre d'une sous-traitance.*** Dans les contrats de cloud computing, il est fréquent que la prestation de services de cloud computing soit exécutée par un tiers au contrat principal formalisé dans le cadre d'un contrat de sous-traitance. Pour engager la responsabilité de ces professionnels (prestataire principal, sous-traitant), il existe une différence de nature d'action selon qu'elle est exercée à l'encontre du prestataire ou du sous-traitant. Lorsque le client, personne morale, souhaite exercer une action judiciaire à l'encontre de son prestataire de services cloud, la nature de l'action en responsabilité est contractuelle dans la mesure qu'ils sont liés par un contrat de cloud computing et que le manquement reproché concerne une obligation contractuelle[1611]. En revanche, lorsque le client, personne morale, souhaite exercer une action judiciaire à l'encontre du sous-traitant, la nature de l'action en responsabilité est délictuelle, dans la mesure qu'ils ne sont liés par aucun contrat. Il s'agit d'une règle de jurisprudence constante depuis l'arrêt BESSE de la Cour de cassation [1612]. En l'espèce, notre attention est portée sur la mise en jeu de la responsabilité contractuelle du prestataire. Il est, par exemple, possible de prévoir dans le contrat que c'est le prestataire qui est responsable de la bonne exécution du contrat que les obligations soient exécutées par lui ou son sous-traitant. Il s'agit de pouvoir renforcer le contrat par des clauses qui imposent au prestataire des obligations une obligation de s'assurer de la bonne exécution des obligations du contrat, telles que l'obligation de sécurité. Afin de renforcer le droit à réparation conventionnel du client en cas d'atteinte à ses données, il est proposé d'intégrer une clause générale relative à l'engagement de la responsabilité contractuelle et de ses effets.

***691.*** À ce titre, il est présenté, ci-après, une proposition de clause générale relative à l'engagement de la responsabilité contractuelle du prestataire et son (ses) sous-traitant(s) : « Le Prestataire est responsable de plein droit à l'égard du Client de la bonne exécution des obligations résultant du contrat et de ses annexes, que ces obligations soient à exécuter par lui-même ou par son (ses) sous-traitant(s). Le prestataire de service cloud s'engage à se conformer aux obligations stipulées dans le contrat et ses annexes et à s'assurer du respect de ces obligations lorsqu'une partie ou l'intégralité de la prestation, objet du contrat, est confiée à un tiers au contrat. En cas de contravention à l'une des obligations prévues au contrat et ses annexes par lui-même et/ou son (ses) sous-traitant(s), le Prestataire s'engage à réparer l'intégralité des préjudices subis par le Client qui résulteront de cette atteinte sans opposer une quelconque limitation de responsabilité. À ce titre, le prestataire s'engage à verser au profit du Client une indemnisation compensatrice d'un montant équivalent à X % du montant du

[1611] V. art. 1103, 1193 ou 1194 du Code civil (ancien article 1134).

[1612] V. Cass, Ass. Plén. du 12 juillet 1991, pourvoi n° 90-13.602 : La Cour a considéré que l'action en responsabilité contre le sous-traitant est de nature délictuelle et non contractuelle.

préjudice évalué. En cas de désaccord sur l'évaluation du montant du préjudice, il est possible pour l'une ou l'autre des parties de faire appel à une expertise. Le Prestataire peut s'exonérer de tout ou partie de sa responsabilité en apportant la preuve que l'inexécution ou la mauvaise exécution du contrat est imputable soit au Client, soit au fait, imprévisible et insurmontable, d'un tiers étranger (hormis son (ses) sous-traitant(s)) à la fourniture des prestations prévues au contrat, soit à un cas de force majeure ».

***692.*** Si l'ingénierie contractuelle permet de renforcer le droit à réparation en cas de manquements du prestataire à ses obligations conventionnelles de protection des données par la mise en jeu de la responsabilité, il apparaît nécessaire de prévoir, en outre, des prévisions contractuelles relatives à l'extraterritorialité.

**2) Le renfort des prévisions contractuelles en matière d'extraterritorialité**

***693. La détermination conventionnelle de la loi applicable et la compétence juridictionnelle.*** La question du droit applicable et de la compétence juridictionnelle suscite une attention particulière dans le cadre de l'exécution d'un contrat de cloud computing en raison que les services s'exécutent dans un contexte international[1613]. Hors hypothèse d'un contrat d'adhésion, le client, personne morale, pourra demander au prestataire de services cloud d'introduire, dans le contrat de cloud computing, des clauses relatives à la loi applicable et à la compétence juridictionnelle qui lui soient profitables. Afin de limiter les risques de l'application d'une loi étrangère au contrat, il est conseillé de prévoir une clause relative au droit applicable qui soumet le contrat cloud au respect de la réglementation nationale. En principe la rédaction d'une clause de droit applicable ne présente pas de difficultés rédactionnelles ; il est proposé, ci-après, une proposition de clause concernant le droit applicable : « Le présent accord ainsi que ses annexes sont soumis à la réglementation française en vigueur »[1614]. Outre la clause relative à loi applicable, il est fondamental de prévoir dans le contrat de cloud computing, une clause relative à la compétence juridictionnelle afin d'éviter tout aléa juridique. À titre illustratif, il est proposé, ci-après, une clause relative à la compétence juridictionnelle : « En cas de différend entre le Prestataire et le Client professionnel, la compétence juridictionnelle est attribuée expressément aux tribunaux français territorialement et matériellement compétents, nonobstant pluralité de défendeurs ou appel en garantie, y compris pour les mesures d'urgence, conservatoires en référé ou sur requête ». L'insertion dans le contrat cloud attribuant la compétence juridictionnelle aux tribunaux français permet, ainsi, de renforcer l'effectivité de clause relative à l'application de la

[1613] V. *supra* n°164.

[1614] V. *supra* n° 233 concernant la clause relative au droit applicable.

loi française au contrat et contribue, ainsi, au renforcement de la protection des données de la personne morale.

***694. La résolution d'un conflit entre les Conditions générales et les Conditions particulières du contrat cloud.*** Dans les contrats conclus entre des personnes morales, si le principe est la liberté contractuelle concernant la détermination du droit applicable et l'attribution de la compétence juridictionnelle, il peut arriver un conflit entre les Conditions générales et les Conditions particulières du contrat cloud. Dans cette configuration, la question se pose de savoir quel document contractuel prime par rapport à l'autre. En pratique, le principe est celui de la primauté des conditions particulières sur les conditions générales en raison que les premières sont considérées comme étant plus spécifiques à l'opération contractuelle. Pour parfaire la sécurisation juridique, il est conseillé d'intégrer conventionnellement cette primauté afin d'éviter tout débat en cas de différend porté devant une juridiction. En effet, il existe un risque à ce que « que des juges, pour faire prévaloir une clause générale dont ils trouvent subjectivement l'effet plus juste, décident que la condition particulière n'était pas suffisamment claire pour écarter effectivement la clause générale qu'elle venait contredire »[1615]. Il est repris, ci-après, une proposition de rédaction de clause : « Au cas de divergence ou de contradiction entre les conditions particulières et les conditions générales, les premières l'emporteront » [1616].

***695. La protection du patrimoine informationnel par la clause du droit applicable et de la compétence juridictionnelle***. L'intégration des clauses de droit applicable et de compétence juridictionnelle dans le contrat de cloud computing a pour objet de sécuriser le contrat en cas de différend entre le prestataire et le client. En effet, il est plus protecteur pour un client, personne morale, d'agir en justice contre son prestataire lorsque la compétence juridictionnelle est dévolue aux tribunaux français et que la loi applicable au contrat est la réglementation française. Si, au contraire, ce sont des tribunaux étrangers qui sont compétents et que la loi applicable est la réglementation étrangère, alors le client pourra est mis en difficulté pour défendre ses droits en cas d'atteinte à son patrimoine informationnel.

***696. Une vigilance en présence d'un acte étranger ayant une portée extraterritoriale***. En revanche, si le principe est la liberté contractuelle concernant la détermination du droit applicable et l'attribution de la compétence juridictionnelle, il peut arriver, à l'instar des contrats conclus avec des personnes physiques, que ces clauses soient remises en cause en présence d'un

[1615] Testu F.X, Dalloz référence Contrats d'affaires, chapitre 21 – Négociation et conclusion des contrats, édition 2010.

[1616] Ibid.

acte ayant une portée extraterritoriale émanant d'un État étranger[1617]. Dans cette situation, il existe un risque de conflits de lois émanant de deux états différents qui prétendent s'appliquer au contrat cloud. À titre illustratif, il peut exister un conflit de lois entre la réglementation européenne et la réglementation étasunienne dont chacune a une portée extraterritoriale. Concernant les difficultés liées à l'exécution du contrat de cloud dans un contexte international, il est renvoyé aux développements ci-dessus qui ont porté sur la détermination conventionnelle de la loi applicable et la compétence juridictionnelle[1618], l'importance de la nationalité du prestataire et de la localisation des données sur le droit applicable et la compétence juridictionnelle[1619], les propositions doctrinales pour contrer l'extraterritorialité judiciaire[1620].

***697.*** Après avoir envisagé le renforcement de la protection des données par la sécurisation conventionnelle, il est proposé de l'envisager à présent, par une alliance de la technologie et du contrat.

## Section 2 : Le renforcement de la protection des données par l'alliance de la technologie et du contrat

***698. La nécessaire sécurité du patrimoine informationnel par les mesures techniques de protection.*** Dans le cadre d'un contrat de cloud computing, il est mis l'accent sur l'exigence de sécuriser ce patrimoine informationnel depuis sa création et pendant toute la période d'hébergement dans l'infrastructure en nuage. Pour évaluer le niveau de sécurité du patrimoine informationnel, il est fait emploi dans les contrats de cloud computing des critères d'audit de sécurité regroupés sous l'acronyme DICP (Disponibilité, Intégrité, Confidentialité, Preuve/traçabilité)[1621]. La disponibilité correspond à « la capacité d'un système d'information à pouvoir être utilisé à tout moment en fonction des performances prévues »[1622]. L'intégrité fait référence à « la propriété qui assure qu'une information n'est modifiée que par les utilisateurs habilités dans les conditions d'accès normalement prévues »[1623]. Il apparaît que cette exigence

[1617] V. *supra* n° 211 et suivants concernant la mise en œuvre des lois sécuritaires des USA.

[1618] V. *supra* n° 686 relatif à la détermination conventionnelle de la loi applicable et la compétence juridictionnelle.

[1619] V. *supra* n° 365 relatif à l'importance de la nationalité du prestataire et de la localisation des données.

[1620] V. *supra* n° 366 relatif aux propositions doctrinales pour contrer l'extraterritorialité judiciaire.

[1621] Livre blanc du CIGREF -FedISA, Protection du patrimoine informationnel, 30 novembre 2007 : il est mis en avant la nécessité de protéger le patrimoine informationnel de l'entreprise en ce qu'il a une forte valeur financière au titre de l'actif immatériel de l'entreprise.

[1622] Ibid.

[1623] Ibid.

de sécurisation technique du patrimoine informationnel est fondamentale en particulier lorsque ce patrimoine figure dans une infrastructure en nuage. En l'espèce, il s'agit de pérenniser la sécurité technique au travers de l'élaboration de clauses spécifiques. Cette partie est, ainsi, dédiée au renforcement de la protection des données par l'intégration de clauses relatives à la sécurité dans le contrat de cloud computing.

***699. L'intégration de la sécurité technique dans le contrat de cloud computing.*** En matière de sécurité, « il apparaît que c'est le prestataire qui fournit au client sa politique standard de sécurité, souvent non contractuelle. Le client doit vérifier que cette politique répond bien à ses propres exigences en matière de protection des données. La discussion portera alors sur le caractère contractuel (et donc engageant) de ces règles, pour lesquelles il conviendra que le client demande *a minima* qu'elles soient annexées au contrat »[1624]. Ainsi, en matière de sécurité des données du client, la négociation des contrats cloud prend tout son sens. La question se pose, ici, de savoir comment intégrer efficacement des clauses relatives à la sécurité pour renforcer la protection des données. Il apparaît que les clauses de sécurité dans les contrats cloud sont déterminées de manière distincte en fonction qu'il s'agisse de la sécurité des données hébergées ou de la sécurité de l'infrastructure. Également, il s'agira d'observer de quelle manière les mesures techniques sont intégrées dans le champ contractuel.

***700.*** **Plan.** Il s'agit d'étudier les clauses qui traitent de la sécurité de l'infrastructure au travers de mesures techniques : les sauvegardes, les contrôles d'accès, le chiffrement (A) et de la réversibilité des données (B).

## A) Le renforcement de la protection des données par les clauses relatives aux mesures techniques

***701.*** **Plan.** Il est procédé à l'étude de la répartition des obligations de sécurité (1) suivi des mesures techniques garanties par le prestataire de services cloud (2).

### 1) La répartition des obligations de « sécurité » dans le contrat de cloud computing

***702.*** Dans les contrats de cloud computing ou dans les politiques de sécurité du prestataire de services de cloud computing, il apparaît une distinction entre la sécurité des données et la sécurité de l'infrastructure.

[1624] Chavernoz A. et Goupil C., Contrats cloud : quels points d'attention dans la négociation ? La Semaine Juridique Edition Générale n° 23, 7 juin 2021, 627.

***703.*** **Plan.** Il sera, donc, envisagé d'étudier la répartition des obligations de sécurité dans le contrat cloud en distinguant la sécurité des données hébergées dans le cloud par le client (a) et la sécurité de l'infrastructure cloud (b).

a) Les données hébergées dans le cloud, une sécurité assurée par le client

***704.*** ***L'intégration de l'obligation de sécurité des données du client dans le contrat.*** Dans le cadre d'une analyse des contrats de cloud computing, une distinction est opérée entre la sécurité de l'infrastructure cloud et la sécurité de la donnée. Il est, en principe, précisé dans les contrats de cloud computing que la sécurité des données hébergées dans le cloud est de la responsabilité du client. C'est ainsi que dans les engagements du prestataire de services cloud de la société OVH, il est rappelé concernant la répartition des actions de sécurité à mettre en œuvre, que « le client est seul responsable de la sécurisation des ressources et des systèmes applicatifs qu'il déploie dans le cadre de l'utilisation de nos services (cloud) »[1625]. Dans le contrat de cloud computing, il est primordial de déterminer et d'encadrer cette obligation de sécurité des données et la responsabilité en découlant. En principe, il est prévu dans le contrat cloud que la sécurité des données hébergées dans le cloud est une obligation à la charge du client. Ainsi, « au-delà de son obligation classique de collaboration avec le prestataire et de celle de payer le prix de la prestation de service, le client est soumis à quelques obligations et responsabilités particulières lorsqu'il s'engage dans un contrat de cloud computing »[1626]. Il incomberait, alors, au client, de mettre en œuvre une politique stricte de gestion des mots de passe.

***705.*** Dans la plupart des cas, il est stipulé au contrat cloud que le client est responsable des dommages subis lorsqu'il a manqué à son obligation de sécuriser les données. Cette responsabilité est à la charge du client puisque dans le cadre de l'exécution d'un contrat de cloud computing, il conserve « la maîtrise » du chargement et du traitement de ses données dans le cloud. En effet, le client est reconnu comme conservant le « contrôle » sur les actions prises dans la gestion de son espace cloud. Le client a, ainsi, l'obligation contractuelle de sécuriser ses données dans le cloud. Dans cette configuration, le client ne pourra pas demander au prestataire de services cloud de réparer les dommages subis dès lors que la réalisation du dommage provient du manquement du client à son obligation de sécuriser ses données.

[1625] OVH et la protection des données à caractère personnel, 3, les engagements d'OVH en matière de sécurité, page 5 : https://www.ovh.com/fr/files/2018-06/plaquette-gdpr-web-Final-French.pdf

[1626] Warusfel B. (sous la direction de Vivant M.), Le Lamy droit du numérique 2018, Expert, Partie 3 - Numérique et contrats, division 3 - Les principaux contrats du numérique et leurs spécificités, chapitre 6 - Les contrats d'informatique dématérialisée (cloud computing), p.491 n°705, mis à jour 22 avril 2022.

***706.*** C'est ainsi que certains prestataires de services cloud (tel qu'Amazon) mettent expressément à la charge de leurs clients une obligation de sécuriser les données[1627]. Il est mentionné que le client a la responsabilité de veiller à la sécurité de son compte et de ses données et d'assurer des sauvegardes. À titre d'exemple, il est stipulé que le client est « seul responsable de l'application des mesures de sécurité appropriées à vos données et de votre utilisation des médias, des appareils et des matériaux de snowmobile, y compris le chiffrement des données sensibles et de ne pas autoriser l'accès non autorisé aux médias, aux appareils ou aux matériaux de snowmobile »[1628].

***707.*** Au regard des effets de ces clauses quant à une exclusion de responsabilité du prestataire, il convient de s'interroger si l'imposition de cette obligation conventionnelle de sécurité des données par le prestataire de cloud computing à la charge du client, personne morale, est légitime. Pour cela, il est proposé de s'appuyer sur une analyse de la qualification juridique du contrat de cloud computing.

***708. Une obligation de sécurité des données à la charge du client justifiée par la notion de « maitrise ».*** Le client, personne morale, utilise un espace virtuel pour stocker ses données. La prestation d'hébergement des données est considérée comme étant « une prestation inhérente au contrat infonuagique – caractérisée par la mobilité des données traitées et le caractère distant des moyens servant à ce traitement »[1629]. Le prestataire met, ainsi, à la disposition du client, personne morale, un espace de stockage de données et éventuellement d'applications de logiciels. Il convient de procéder à la qualification juridique du contrat cloud intégrant la prestation d'hébergement afin d'apprécier la légitimité de l'obligation de sécurité des données à la charge du client. La doctrine, à ce titre, propose les qualifications suivantes : le contrat de location, le contrat de dépôt, le contrat d'entreprise[1630]. Il est procédé, alors, à une analyse de la légitimité de cette obligation au regard de chacune de ces contrats.

---

[1627] Dans le contrat client AWS , il est énoncé qu'il incombe au client « de configurer et d'utiliser correctement les Offres de Services et de prendre toutes autres mesures adéquates afin de sécuriser, protéger et sauvegarder vos comptes et votre Contenu, de manière à assurer une sécurité et une protection appropriées, notamment en recourant à une technologie de cryptage visant à protéger Votre Contenu de tout accès non autorisé et archiver régulièrement Votre Contenu » : https://d1.awsstatic.com/legal/aws-customer-agreement/AWS_Customer_Agreement-FR_(2019-04-30).pdf.

[1628] Contrat cloud AWS : https://d1.awsstatic.com/legal/awsserviceterms/AWS%20Service%20Terms%20%20French%20Translation.pdf.

[1629] Précision sur les prestations d'hébergement : « L'hébergement : une prestation inhérente au contrat infonuagique – Caractérisées par la mobilité des données traitées et le caractère distant des moyens servant à ce traitement, les solutions infonuagiques incluent par essence une prestation d'hébergement. Celle-ci consistera pour le fournisseur, à mettre à la disposition du client, un espace de stockage pour y accueillir, selon le cas, soit des données (à des fins d'archivage par exemple), soit des données accompagnées d'une ou plusieurs application(s) logicielle(s), permettant leur traitement (généralement aux fins de réalisation d'une ou plusieurs tâche(s) métier) » : Bourgeois M., JurisClasseur Communication, Fasc. 962 : cloud computing – Les défis contractuels du Cloud Computing, 1er Mai 2020.

[1630] V. *supra* n° 29 et suivants relatifs à la qualification du contrat cloud.

***709.*** Si nous retenons la qualification de contrat de location, il apparaît légitimé de faire peser l'obligation de sécurité des données sur le client en raison qu'il dispose la maîtrise sur ses données. Il a le contrôle des accès aux serveurs (avec la mise en place de mots de passe) et a la possibilité d'exercer plusieurs prérogatives telles qu'ajouter des données, les supprimer, les déplacer (..). En outre, s'agissant de la sécurité de l'infrastructure cloud, celle-ci est à la charge du prestataire en raison qu'il conserve la « maitrise » de ses serveurs. Il en résulte qu'il existe une distinction entre obligation de sécurité des données et obligation de sécurité de l'infrastructure, dont la première incombe au client et la seconde au prestataire.

***710.*** Cette distinction est pertinente, également, dans le cadre d'un contrat de dépôt et d'un contrat d'entreprise. Dans le contrat de dépôt, le client a, certes, l'absence de maîtrise sur le dépôt, tel que la connaissance de l'endroit du dépôt [contrat de dépôt] ; en revanche, il est possible de considérer qu'il dispose de la maîtrise de la chose déposée avec la faculté par exemple de la récupérer. De la même manière dans le contrat d'entreprise, le client n'a pas la maîtrise concernant la réalisation des prestations de services objet d'un contrat de cloud computing, mais garde la maîtrise sur les données dans la mesure qu'un contrat de cloud computing (incluant par nature une prestation d'hébergement) a pour objet de mettre « à la disposition du client, un espace de stockage pour y accueillir, selon le cas, soit des données (à des fins d'archivage par exemple), soit des données accompagnées d'une ou plusieurs application(s) logicielle(s), permettant leur traitement [généralement aux fins de réalisation d'une ou plusieurs tâche(s) métier] »[1631]. Cet objet du contrat de cloud implique donc « que toute donnée qu'il crée via l'utilisation du service reste la "propriété" du client. Au terme fixé du contrat, le client doit pouvoir avoir accès au service afin de récupérer son contenu : ce droit de retrait sans limitation paraît légitime [ces données sont celles du client] et essentiel dans la logique d'un monde cloud fourni en "marchandises" *[commodity]* substituables. De même, le prestataire s'engage en principe à n'utiliser les données du client que pour les besoins de la fourniture du service et de sa maintenance »[1632]. Il résulte de cette analyse que, peu importe la qualification retenue (contrat de location, contrat de dépôt ou contrat d'entreprise), la clause retranscrivant l'obligation de sécurité des données du client est considérée comme valide en raison que ce dernier conserve la maîtrise sur les données qu'il héberge dans le cloud. Dès lors que le client dispose la maîtrise sur les données, il doit pouvoir être en mesure de protéger ses données notamment par la mise en place d'un contrôle et d'un accès restreint aux serveurs.

[1631] Ibid.

[1632] Chavernoz A. et Goupil C., Contrats cloud : quels points d'attention dans la négociation ? La Semaine Juridique Edition Générale n° 23, 7 juin 2021, 627.

***711. L'intégration de la prévision contractuelle relative à la sécurité des données.*** Si l'obligation de sécurité des données à la charge du client est légitime[1633], en quoi cette prévision contractuelle pourrait contribuer au renforcement de la protection des données de la personne morale dans les contrats de cloud computing ? L'intégration dans le contrat cloud de cette clause permet de renforcer la protection des données de la personne morale dans la mesure que celle-ci informe le client de ses obligations et lui permet ainsi d'être acteur [corrélativement responsable] de la protection de ses données hébergées dans le cloud en s'assurant de la sécurité de ses données (mise en place de mots de passe, sauvegarde des données...). Pour que cette clause puisse être effective et être favorable à un renforcement de la protection des données des personnes morales, encore faut-il s'assurer que cette clause soit communiquée au client [délivrance de l'information] et qu'elle soit rédigée de manière expresse, claire et sans équivoque. À ce titre, il est présenté, ci-après, une proposition de clause relative à une obligation de sécurité des données à la charge du client :

« Pour assurer la sécurité des données hébergées dans le cloud computing, il est mis à la charge du Client une obligation de sécuriser l'accès à ces données hébergées dans le cloud computing. Il incombe au Client de prendre toutes les mesures nécessaires et appropriées pour sécuriser ses données, telles qu'un accès restreint à certaines personnes et l'établissement de mots de passe pour accéder au serveur. En cas de négligence avérée par le Client concernant son obligation de sécurité des données, le prestataire ne sera pas tenu pour responsable ». Par l'intégration de cette clause expresse et non équivoque, le client est, ici, au même titre que le prestataire, acteur de la protection de ses données.

***712.*** Corrélativement à cette obligation de sécurité des données du client, il est mis à la charge du prestataire une obligation de sécurité de l'infrastructure cloud en raison qu'il conserve, pendant toute la durée de l'exécution du contrat de cloud computing, la « maitrise » de ses serveurs. Cette clause relative à l'obligation de sécurité de l'infrastructure cloud retranscrite dans le contrat de cloud computing est étudiée dans le développement suivant.

b) L'infrastructure cloud, une sécurité assurée par le Prestataire

***713.*** L'infrastructure cloud appartenant au prestataire, il est évident que le client, personne morale, ne dispose d'aucune maîtrise sur celle-ci ; c'est le prestataire qui la détient. Il apparaît que le contrat de cloud computing prévoit une obligation de l'infrastructure cloud à la charge du

[1633] V. *supra* n° 701 relatif à l'obligation de sécurité des données à la charge du client.

prestataire. Cette exigence de sécurisation de l'infrastructure cloud est mentionnée expressément dans le contrat de cloud computing. À titre illustratif, il est précisé que la société OVH « s'engage à sécuriser ses infrastructures de manière optimale »[1634]. Cette déclaration permet de rappeler aux clients, le principe selon lequel le prestataire de services cloud est responsable en cas de « faille » dans la sécurité des infrastructures. Il est prévu, ainsi, au contrat de cloud computing, les dispositions relatives aux actions et aux mesures de sécurité assurées par le prestataire de services. À titre d'exemple, il est mentionné que « nous avons notamment mis en place une politique de sécurité des systèmes d'information (PSSI) et nous répondons aux exigences de plusieurs normes et certifications : certification PCI-DSS, certification ISO/IEC 27001, attestations SOC 1type 2 et SOC 2 type 2, etc. Nous disposons aussi d'un agrément pour l'hébergement de données de santé (HDS) pour notre offre Healthcare »[1635]. Pour se conformer à cette obligation de sécurité de l'infrastructure, il incombe au prestataire de mettre en œuvre des mesures techniques de protection et en cas de manquement, il engage sa responsabilité.

***714. L'intégration d'une prévision contractuelle relative à la sécurité de l'infrastructure cloud.*** C'est parce qu'il existe des menaces inhérentes à l'utilisation de la technologie du cloud que les parties intéressées par un contrat cloud prennent toutes les mesures nécessaires à la protection de leurs données et prévoient des clauses spéciales relatives à la sécurité de l'infrastructure. La sécurisation technologique, dans le cadre d'un service permanent et continu, permet, par l'emploi des mesures techniques, d'assurer la sécurité à l'entrée dans le réseau cloud. L'objectif du déploiement de ces mesures techniques est de bloquer toute intrusion dans le réseau et prévenir les risques de violations des données. Il apparaît, ainsi, fondamental à ce que le contrat cloud intègre ces garanties techniques permettant de se prémunir contre toute atteinte, telle que l'intrusion de tiers « des pirates » dans le réseau (piratage informatique). Il est proposé, ci-après, un modèle de clause qui encadre l'obligation de sécurité de l'infrastructure cloud à la charge du prestataire :

***715.*** « Pendant toute la durée du contrat, le prestataire s'engage à assurer la sécurité de ses infrastructures en nuage. Le Prestataire informe le Client que les serveurs hébergeant ces données disposent d'une sécurité d'accès et d'un accès physique restreint et sélectif du bâtiment. À ce titre, le prestataire s'engage à mettre en œuvre des mesures de sécurité technique et organisationnelle pour assurer la sécurité de l'infrastructure cloud, telle que des mesures de

[1634] Illustration dans le contrat de cloud computing de la société OVH : « OVH et la protection des données à caractère personnel, 3, les engagements d'OVH en matière de sécurité, page 5 : https://www.ovh.com/fr/files/2018-06/plaquette-gdpr-web-Final-French.pdf.

[1635] Ibid.

chiffrement, des mesures permettant d'assurer la confidentialité, l'intégrité, la disponibilité et la résilience permanentes des systèmes et services de traitement, des mesures d'identification et d'autorisation des utilisateurs, des mesures de protection des données lors de la transmission, les mesures de protection pendant le stockage. Est annexé au présent contre, un document technique qui énumère les mesures techniques mises en œuvre par le Prestataire pour assurer la sécurité de l'infrastructure cloud ». Il est envisagé d'étudier, dans la partie suivante, les garanties techniques mises en œuvre par le prestataire.

***716.*** Après avoir déterminé le principe de l'obligation de sécurité de l'infrastructure cloud à la charge du prestataire de cloud computing, il est envisagé d'étudier les garanties techniques pour le renforcement de la protection des données de la personne morale.

**2) les mesures techniques garanties par le prestataire de services cloud**

***717. L'intégration d'une prévision contractuelle relative aux mesures techniques.*** En exécution de son obligation de sécurité de l'infrastructure cloud, le prestataire de services doit s'assurer de la sécurité de ses centres d'hébergement (datacenters) en mettant en place des mesures techniques de sécurité contre certaines menaces. Pour se prémunir contre une intrusion de tiers dans l'infrastructure cloud, le prestataire doit mettre en place, par exemple, des dispositifs de contrôles d'accès physique, logique, des antivirus (..), contre le feu et les inondations, il devra installer des détecteurs ; contre les pannes électriques, il devra prévoir des alimentations de relais afin de ne subir aucune panne de courant et donc de perte de données. Au niveau de la doctrine, certains auteurs ont rapproché ces diverses obligations à celle de l'obligation de garde qui est mis à la charge du dépositaire[1636], laquelle comprend une obligation de surveillance[1637]. En matière de contrat de cloud computing, cette obligation de surveillance ou « monitoring » en anglais, consiste à exiger du fournisseur qu'il mette en place des processus de sécurisation de l'infrastructure cloud (détection des menaces ou dysfonctionnements) et doit immédiatement (ou dans les meilleurs délais) en alerter le client. À titre d'exemple de mesures techniques garanties par le prestataire dans le contrat de cloud computing, il est précisé dans le contrat de cloud computing de la société OVH que « pour l'ensemble de ses services, OVH s'engage à mettre en place : des mesures de sécurité physique afin d'empêcher l'accès aux infrastructures

[1636] Bourgeois M., JurisClasseur Communication, Fasc. 962 : cloud computing – Les défis contractuels du Cloud Computing, 1er Mai 2020 – v. C. civ., art. 1927 à 1937.

[1637] Cass. com., 9 févr. 2016, n° 14-23.006 : JurisData n° 2016-002016 : la banque qui met un coffre-fort à la disposition d'un client est tenue d'une obligation de surveillance qui lui impose d'établir qu'elle a accompli toutes les diligences utiles, pour en contrôler l'accès par un tiers, et qui est appréciée avec plus de sévérité lorsque le contrat est conclu à titre onéreux (C. civ., art. 1928).

par des personnes non autorisées ; un personnel de sécurité chargé de veiller à la sécurité physique de nos locaux 24 heures sur 24 et 7 jours sur 7 ; un système de gestion des permissions permettant de limiter l'accès aux locaux et aux données aux seules personnes habilitées, dans le cadre de leurs fonctions et de leurs périmètres d'activité ; un système d'isolation physique et/ou logique (selon les services) des clients entre eux ; des processus d'authentification forts des utilisateurs et administrateurs grâce, notamment, à une politique stricte de gestion des mots de passe et au déploiement de certaines mesures de double authentification comme YubiKey ; des processus et dispositifs permettant de tracer l'ensemble des actions réalisées sur notre système d'information et d'effectuer, conformément à la réglementation en vigueur, des rapports en cas d'incident affectant les données de nos clients »[1638]. De la même manière, Amazon, précise dans son contrat cloud AWS qu'Amazon instaure des mesures raisonnables et adaptées pour sécuriser le contenu (les données) à l'encontre de toute perte, d'accès ou divulgation accidentel (le) ou illégal(e)[1639]. Dans les conditions du contrat cloud d'Apple, il est précisé qu'« Apple a mis en place "des protocoles de chiffrement comme Transport Layer Security (TLS) pour protéger vos renseignements (..) pendant le transit », que les données sont stockées « dans des systèmes informatiques à accès limité, hébergés dans des installations où des mesures de sécurité physiques sont en place et sont cryptées avant d'être stockées »[1640]. Dans le contrat cloud de Google, il est mentionné que Google promeut auprès de ses clients, personnes morales, les moyens technologiques permettant d'assurer la sécurité et la confidentialité des données des utilisateurs de services cloud ; que la sécurité fait partie intégrante des services cloud et que tous les produits Google intègrent de puissantes fonctionnalités de sécurité[1641].

***718. La mise en œuvre d'une diversité de mesures techniques.*** Il en résulte de l'analyse de ces dispositions contractuelles que plusieurs mesures de sécurité sont mises en œuvre pour se prémunir contre tout accès, toute modification, divulgation ou destruction non autorisée des données. Ces mesures de sécurité sont, notamment , le chiffrement des données[1642] afin d'en garantir la confidentialité, la navigation sécurisée, la vérification ("Check-up" en anglais), la sécurité et la validation en deux étapes, les audits internes sur la collecte, le stockage et le traitement des données, y compris les mesures de sécurité physiques afin d'empêcher tout accès

[1638] Clause 4- Obligations d'OVH – contrat de cloud computing V. également, OVH et la protection des données à caractère personnel, 3, les engagements d'OVH en matière de sécurité, page 5 : https://www.ovh.com/fr/files/2018-06/plaquette-gdpr-web-Final-French.pdf.

[1639] Contrat client D'Amazon Web Services (AWS) (https://d1.awsstatic.com/legal/aws-customer-agreement/AWS_Customer_Agreement-FR_(2019-04-30).pdf).

[1640] Contrat i.cloud d'Apple, politique de confidentialité : https://www.apple.com/legal/privacy/fr-ca/.

[1641] Contrat cloud de Google : https://policies.google.com/terms.

[1642] V. *supra* n° 63 concernant la définition du chiffrement.

non autorisé aux systèmes »[1643]. Afin de renforcer la protection des données stockées dans le cloud, le prestataire de services cloud prévoit des mesures techniques de sécurisation de l'infrastructure cloud, car il en est de sa responsabilité. Le détail des mesures techniques de sécurité permet au prestataire de services cloud d'être en mesure de justifier auprès des autorités de contrôles (ANSSI et CNIL) le respect des obligations relatives à la sécurité[1644].

***719.*** L'intégration de ces clauses relatives à la sécurité technique dans le contrat de cloud computing témoigne la préoccupation du prestataire de sécuriser l'infrastructure cloud. Seulement, très souvent, ce sont des clauses déclaratives et le client n'est jamais en mesure de vérifier l'effectivité de ces clauses. En revanche, ces déclarations sont renforcées lorsqu'elles s'appuient sur des certifications attestant le niveau de sécurité des mesures techniques déployées par le prestataire pour sécuriser l'infrastructure.

***720. La clause de l'audit de contrôle à double tranchant*** : En outre, il est conseillé une clause relative à la réalisation d'audit pour contrôler la conformité des mesures techniques aux prévisions contractuelles. À ce titre, il est reproduit, ci-après, la clause d'audit proposé dans un ouvrage :

« Le prestataire et les services qu'il fournit pourront faire l'objet d'audits qui auront notamment pour but de vérifier : a. le respect de la convention de niveau de services — SLA (Service Level Agreement) ; b. que le Prestataire se conforme aux procédures et aux normes de sécurité définies à l'article XX ; c. que le Prestataire respecte les obligations qui lui incombent en vertu de l'article XX ; d. que les moyens et les procédures mis en œuvre par le Prestataire sont conformes au plan de gestion des désengagements, comme indiqué à l'article XX ; e. et s'assurer que l'ensemble des documents comptables obligatoires et des données à collecter en vertu des lois et règlements applicables existe, est mis à jour conformément aux méthodologies généralement admis et, d'une façon générale, selon des modalités et avec un niveau de détail suffisants pour justifier le calcul des charges liées aux services. Le Prestataire est tenu de conserver tous les documents et pièces justificatives nécessaires pendant la durée du contrat et, au-delà pendant le délai prévu par les politiques du Client telles qu'elles ont été notifiées au Prestataire ou, à défaut, conformément aux dispositions du présent contrat et des lois et règlements applicables, étant précisé que le délai retenu ne peut être inférieur à six (6) mois ; f. et mener des investigations conjointes avec le Prestataire, ou identifier les cas présumés de

[1643] Contrat cloud de Google : https://policies.google.com/terms.

[1644] Obligation de mettre en place des mesures techniques : « (…) le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (…) » : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679.

fraude ou d'erreur comptable significative »[1645]. Si cette clause permet au client de vérifier, par la mise en œuvre d'audit, du respect par le prestataire de services cloud de ses engagements contractuels en matière de sécurité ; il faudra veiller, en revanche, à ce que le nombre d'audits ne soit pas opposable en cas de survenance d'un problème technique pour déresponsabiliser le prestataire de services cloud.

***721.*** Il résulte de cette analyse contractuelle que l'intégration des clauses relatives à la sécurité technique de l'infrastructure cloud permet de contribuer au renforcement de la protection des données. Par ailleurs, la sécurité technique au travers des mesures techniques passe aussi par la garantie d'un droit à la réversibilité des données au profit du client, personne morale (ou du portage).

## B) Le renforcement de la protection des données par la clause relative à la réversibilité des données ou le portage des données

***722. La prévoyance de la disponibilité des données dans le contrat cloud.*** Quand bien même le client, personne morale, aurait subi un incident tel qu'un vol, une perte des données ou une indisponibilité temporaire des données, il est conseillé de prévoir dans le contrat cloud une clause permettant de garantir la disponibilité des données. Il existe pour cela deux types de clauses ; « la clause de réplication des données » et « la clause de réversibilité des données ». La première envisage de dupliquer « les données sur d'autres sites distants et feront ensuite l'objet d'une restauration dans des délais et modalités prédéfinis »[1646]. La seconde permet « le retour des données chez le client ou leur transfert chez un autre prestataire » et doit prévoir « les conséquences pratiques de la fin du contrat (remise d'une copie des données, modalités de transfert des données, délais, etc.) »[1647]. Afin de renforcer les droits de la personne morale concernant la protection de ses données confidentielles, il est, donc, important de veiller à ce que le contrat cloud puisse prévoir les clauses relatives à la réversibilité vers un autre prestataire.

[1645] Illustration d'une clause d'audit proposée dans l'annexe 3 du guide pratique du GIGREF-IFACI-AFAI, 2013, p. 33.

[1646] Alix P. et Perfetti G., les contrats de cloud computing : les clauses importantes du point de vue des clients, publié le 24 novembre 2012 : https://www.legavox.fr/blog/virtualegis/contrats-cloud-computing-clauses-importantes-10101.html.

[1647] Ibid.

***723. La consécration du « droit de portage » des personnes morales***. Tel qu'observé dans les développements précédents, le RDNP[1648] a consacré à l'article 1er « le portage des données »[1649]. À titre de rappel, le « portage des données » au profit des personnes morales[1650] se fonde non pas sur un texte, mais un code de conduite établi par les prestataires de services. À ce titre, la clause de réversibilité permet d'exercer le « portage des données ». Elle a pour objet de prévoir le sort des données à la fin du contrat. Le contrat cloud doit prévoir les conditions dans lesquelles le client pourra récupérer les données stockées dans le cloud. Celle-ci permet de définir comment le client peut reprendre ou faire reprendre, par un prestataire choisi par lui, ses données, et ce aux charges et conditions du contrat.

***724. La clause de réversibilité versus la restitution des données***. Dans la plupart des services de cloud computing standard, la réversibilité se résume à la restitution des données du client en leur dernier état de sauvegarde avec la fourniture de celles-ci sur un support standard et exploitable pour le client. À la fin du contrat, le prestataire de services cloud s'engage à remettre au « client une copie de l'ensemble des données en format standard, dans leur dernier état de conservation à la date de la demande, et détruit toute copie sur le serveur après information du Client »[1651]. En d'autres termes, dans le cadre d'un service de cloud computing standard, on parle davantage de « restitution des données » que d'une « réversibilité » des données.

***725. La clause de réversibilité versus la véritable réversibilité***. Alors que dans le cadre d'un service de cloud computing qui prévoit des services personnalisés, comme l'intégration de logiciels tiers et de web services additionnels, la réversibilité réapparaît et doit être clairement définie et encadrée dans le contrat. La réversibilité inclut, ici, en plus de la restitution des données dans un support standard exploitable, une prestation d'assistance pour la réalisation de la migration des données et la reprise de logiciels. En outre, la clause de réversibilité détermine les tâches incombant à chacune des parties au contrat dans le cadre d'un plan de réversibilité. En principe, ce type de clause est actionné lorsqu'il y a soit un litige soit au terme du contrat ; il est donc préconisé de la négocier, en amont, au moment de la formation du contrat. Dans cette configuration, cette clause pourra être mentionnée dans l'objet du contrat comme étant une obligation essentielle du contrat. Il s'agit d'une clause importante puisqu'elle concerne la

[1648] Le règlement (UE) numéro 2018/1807 du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne (RDNP), *op. cit.*.

[1649] V. art. 1er du RDNP.

[1650] V. art. 6 du RDNP.

[1651] Guide, Contractualisation des services cloud, les enjeux juridiques, Staub & Associes : https://www.eurocloud.fr/doc/guide-contractuel-cloud.pdf.

récupération des données confidentielles et stratégiques de la personne morale. L'objectif de cette clause est de prévoir la récupération des données sans encombre et éviter, ainsi, de perturber le bon fonctionnement et la continuité de l'activité en cas de pertes ou de détériorations des données. Les clauses relatives à la réversibilité vers un autre prestataire sont requises afin de limiter le risque d'atteinte aux données stratégiques de l'entreprise. En effet, il y a un risque majeur et évident qu'un seul prestataire de services cloud, très souvent non-ressortissant du pays du client, puisse traiter l'ensemble des données de l'entreprise et parmi ces données figurent les données stratégiques lesquelles sont d'une valeur supérieure aux services fournis par le prestataire[1652]. La réversibilité est, donc, un élément essentiel du contrat de cloud computing permettant de garantir à l'utilisateur la reprise du contrôle de ses données avec la coopération technique de son prestataire de services cloud.

***726. L'identification du contenu protecteur de la clause de réversibilité.*** La doctrine identifie le contenu protecteur d'une clause de réversibilité et considère que « la clause de réversibilité devra définir : les délais et modalités de fournitures des données : il faudra prévoir les responsabilités éventuelles en cas de dégradation, perte, d'accès non autorisé et/ou de détournement de fichiers lors de la transmission ; le format du fichier de restitution ; la documentation qui permet d'identifier les données contenues dans le fichier intermédiaire comprenant les données restituées ; la collaboration attendue du client, et ce afin de déterminer les destinataires du fichier de restitution ; les modalités d'assistance complémentaire éventuelle : il faudra définir les délais, les personnes, les coûts et les responsabilités »[1653].

***727. La prévision contractuelle de la réversibilité des données.*** À la suite des observations doctrinales, il est reproduit, ci-après, une clause figurant dans un ouvrage relative à la réversibilité des données : « En cas de cessation des relations contractuelles pour quelque cause que ce soit, le prestataire s'engage à assurer une totale réversibilité des données appartenant au Client, sur le plan technique et à tout mettre en œuvre, sur les plans juridique et humain, afin de permettre au client de reprendre, ou de faire reprendre par un tiers désigné par elle, l'administration des données du client. À ce titre, le Prestataire s'engage à fournir au Client, à sa

[1652] Illustration d'un modèle de clause dans le contrat Cloud de la société IBM laquelle stipule : « A la fin du Contrat, quelle qu'en soit la cause, IBM s'engage à supprimer ou à restituer les données (…) »https://www.ibm.com/support/customer/csol/contractexplorer/cloud/consolidated-agreement/upbdgoqurbgxufr8uhtfta.

[1653] Mallet-Poujol N., Le Lamy droit du numérique, expert, sous la responsabilité de Vivant M., partie 3 Numérique et contratsDivision 3 Les principaux contrats du numérique et leurs spécificités- Chapitre 6 Les contrats d'informatique dématérialisée (cloud computing) - Section 5 Les clauses essentielles des contrats de cloud§ 6. La clause de réversibilité dernière mise à jour 22 avril 2022.

demande, la copie sur < cartouche magnétique > de la dernière situation des données du client. En cas d'expiration ou de résiliation du contrat entre les parties, pour quelque motif que ce soit le Client sera en droit d'obtenir du Prestataire que ce dernier lui communique toutes les informations qui lui seront nécessaires pour lui permettre de préparer la réversibilité des données. Ce droit s'exerce pendant le délai nécessaire à la réalisation de la réversibilité et, au plus tard à l'expiration d'un délai de deux mois à compter de la date de signification de la résiliation ou de la cessation des relations contractuelles pour quelque cause que ce soit. Les parties conviennent des dispositions financières suivantes, en ce qui concerne les prestations d'assistance à la réversibilité fournie par le Prestataire, y compris celles relatives au transfert de données : — si la réversibilité découle d'une résiliation anticipée du présent contrat à la suite d'un manquement du Prestataire, les prestations d'assistance à la réversibilité ne seront alors pas facturées au client ; — si la réversibilité découle de la survenance d'un cas de force majeure, les coûts de l'assistance à la réversibilité supportés par le Prestataire seront partagés par moitié entre les parties ; — si la réversibilité découle de toute autre cause d'interruption du présent contrat, les prestations d'assistance à la réversibilité effectuées par le Prestataire seront facturées au Client dans leur intégralité, sur la base des tarifs du Prestataire en vigueur au jour de la résiliation des prestations, après acceptation d'un devis présenté à ce titre au Client par le Prestataire »[1654]. En complément de celle-ci, il semble opportun d'annexer une clause détaillant l'assistance fournie post-résiliation. À ce titre, il est repris, ci-après, une clause relative à cette période : « En cas d'expiration et/ou de résiliation du Contrat, et dès lors que le client en fait la demande 15 jours au moins avant la date d'expiration et/ou de résiliation du Contrat, le prestataire continuera à fournir les Services pendant une période additionnelle de jours après la date de xx fin du Contrat (« Période de Transition »), selon les mêmes modalités, sous réserve de la signature préalable par le client d'un bon de commande relatif à la poursuite de ces Services. Toute assistance que le prestataire pourrait être amené à fournir au client en dehors de la poursuite des Services pendant la Période de transition sera soumise à la signature préalable par le prestataire et le client d'un contrat de services professionnels et d'un descriptif de services associés. Les termes et conditions du présent contrat continueront à s'appliquer à la fourniture par le prestataire des Services pendant la Période de Transition »[1655]. En raison de son importance, cette clause doit être complétée par un plan de réversibilité lequel doit prévoir selon Monsieur Alterman et Monsieur Perbost « les conditions de remise par le prestataire de l'ensemble des données et informations — sous un format exploitable — nécessaires à une

[1654] Extrait de Contrat ASP, FLDI, n°II.320-5, Le lamy droit du numérique 2018, édition Lamy expert 2018, Wolterz Kluwer, p.494 n°712.

[1655] Martin N. et Auvieux C., article 15, extrait du formulaire ProActa, Lamyline, FII.345-5 Contrat de fourniture de solutions et de prestations informatiques en mode SaaS.

reprise de service par un autre prestataire ou par l'utilisateur »[1656]. Les clauses reproduites permettent, ainsi, d'offrir davantage de protection en raison de leur caractère exhaustif dans la détermination des conditions de la réversibilité. Elles permettent d'éviter tout aléa juridique en ce qui concerne les obligations du prestataire pour assurer la réversibilité des données.

***728. Les sanctions en cas d'entrave au portage et à la réversibilité des données*** : Si le contrat cloud ne prévoit pas de clauses relatives à la réversibilité des données ou qu'il contient des clauses faisant soit obstacle soit limitant l'exercice du portage créant ainsi des entraves au changement de prestataire, la qualification d'abus de position dominante est susceptible de s'appliquer. Dans ce sens, la jurisprudence a considéré « que tous les comportements et toutes les clauses ayant pour effet d'entraver le changement de fournisseur sont susceptibles de recevoir la qualification d'abus de position dominante »[1657]. En cas de refus du prestataire d'exécuter la réversibilité, le client est susceptible d'agir contre le prestataire de services cloud afin de demander l'exécution de cette obligation conventionnelle. La jurisprudence, dans le cadre de l'exécution d'un contrat de cloud computing de type SaaS, a « fait injonction sous astreinte au Prestataire SaaS de fournir au client tous les moyens techniques lui permettant de réaliser l'exportation de ses données hébergées, ou à défaut de lui consentir au-delà de la date de fin du contrat la continuation gratuite du service le temps nécessaire à ce qu'il soit en état de procéder à cette exportation »[1658]. Il en résulte que la jurisprudence attache une importance à ce que la liberté de choix du prestataire au profit du client par la mise en œuvre de la clause de la réversibilité des données soit respectée et sanctionne les entraves à cette liberté réalisées par le prestataire.

[1656] Extrait de Contrat ASP, FLDI, n°II.320-5, Le lamy droit du numérique 2018, édition Lamy expert 2018, Wolterz Kluwer, p.494 n°712.

[1657] Eréséo N., Libre circulation des données et droit de la concurrence (à propos du règlement du 14 novembre 2018 relatif à la libre circulation des données non personnelles), Dalloz IP/IT 2020 p.414. V. également *supra* n° 339 concernant l'abus de position dominante.

[1658] TGI Nanterre, réf., 30 nov. 2021, UMP c/Oracle France, Expertises 2013, pp.358-360.

# Conclusion du chapitre 2

***729. L'ingénierie contractuelle au service du renforcement de la protection du patrimoine informationnel***. Pour renforcer le droit à la protection des données de la personne morale, il a été préconisé d'insérer dans le contrat de cloud computing des clauses relatives à la sécurité juridique, c'est-à-dire celles qui permettent de prémunir le client d'un risque juridique quant à une atteinte à son patrimoine informationnel. Les clauses nécessaires au renforcement de la protection du patrimoine informationnel sont relatives à la confidentialité, aux obligations d'information, de mise en garde, d'une interdiction de l'exploitation des données par le prestataire ainsi que celles relatives à l'engagement de la responsabilité contractuelle. En sus des clauses relatives à la sécurité juridique, il s'agissait d'intégrer également dans le champ contractuel les clauses relatives à la sécurité technique ; en particulier des clauses qui traitent de la sécurité de l'infrastructure par la mise en place de mesures techniques (les sauvegardes, les contrôles d'accès, le chiffrement) et la clause relative à la réversibilité des données (ou du portage des données).

***730.*** L'intégration de ces clauses dans le contrat de cloud computing permet de répondre aux besoins de protection des données des personnes morales dans les contrats de cloud computing et de compenser, dans certains cas, les lacunes légales en matière de protection de données des personnes morales.

# Conclusion du Titre 2

***731. Le développement d'outils juridiques***. En raison de l'absence d'une réglementation spécifique à la protection des données personnelles dans le cloud computing, des outils juridiques et contractuels ont été mis en place pour compenser cette carence et ainsi renforcer la protection des données dans les contrats de cloud computing. Aujourd'hui, ces palliatifs résident dans l'adaptation des réglementations en vigueur et la mise en place de stratégies de sécurisation contractuelle.

***732. L'adaptation de droits à la protection des données dans le cloud***. Tout d'abord, le renforcement de la protection du patrimoine informationnel a été rendu possible par l'adaptation du droit de la propriété intellectuelle et industrielle en fonction du type de données concernés dans le cloud, telle que la protection par le secret spécifique pour protéger le savoir-faire et le secret de fabrique ou par le droit d'auteur et le droit sui generis du producteur de la base des données. Puis, la protection des données confidentielles de la personne a été renforcée par la mise en œuvre du droit commun des affaires ; en particulier depuis la consécration du « secret des affaires » qui a permis d'étendre la protection à l'ensemble des données confidentielles de la personne morale.

***733. La mise en place de stratégies de sécurisation contractuelle.*** Si l'adaptation du droit de la propriété intellectuelle et industrielle ainsi que le droit commun des affaires permet de protéger les données dans le cloud, il est apparu nécessaire de prévoir dans le contrat de cloud l'application de ce ces principes légaux. Pour renforcer la protection des données dans le cadre de l'exécution du contrat de cloud computing, cette étude a préconisé l'intégration de clauses relatives à la sécurité technique et à la sécurité juridique. Il résulte de cette étude que c'est grâce à l'ingénierie contractuelle que la protection des données confidentielles de la personne morale peut être renforcée.

# Conclusion de la Partie 2

***734. Les moyens juridiques et contractuels pour le renforcement de la protection des données.*** Cette étude a consisté à identifier les moyens juridiques permettant de remédier aux lacunes légales, en matière de protection des données dans les contrats de cloud computing, identifiées en première partie. Ces moyens juridiques résident dans l'adaptation de la réglementation en vigueur, la consécration de nouveaux droits et la mise en place d'une stratégie de sécurisation contractuelle.

***735. Le renforcement de la protection des données à caractère personnel.*** Il a été étudié que le renforcement de la protection des données à caractère personnel est rendu possible par la mise en œuvre d'un droit à l'autodétermination informationnelle effectif et par le renforcement du droit à réparation. La consécration dans les textes d'un droit à l'autodétermination informationnelle (issu du droit fondamental à la protection des données à caractère personnel) a conféré au profit de la personne physique, un droit de contrôle et un droit de décision sur l'utilisation de ses données et une diversité de prérogatives. Par la consécration de ce droit à l'autodétermination informationnelle, la personne physique a la capacité de contrôler la divulgation de ses informations personnelles et de décider de leurs utilisations. En outre, la protection des données à caractère personnel a été renforcée par la mise en œuvre du droit à réparation des personnes physiques qui se traduit, en pratique, par un élargissement du champ de la réparation et des responsabilités. Il en résulte que grâce à la mise en œuvre d'un droit à l'autodétermination informationnelle effectif et un élargissement du droit à réparation, la protection des données personnelles des personnes physiques se trouve renforcer dans le cadre de l'exécution d'un contrat de cloud computing.

***736. Le renforcement de la protection des données des personnes morales.*** Il a été fait le choix d'étudier le renforcement de la protection des données des personnes morales (patrimoine informationnel) dans le cadre de l'exécution du contrat de cloud computing au travers de l'adaptation des réglementations en vigueur et de l'ingénierie contractuelle. S'agissant de l'adaptation des réglementations en vigueur à la protection du patrimoine informationnel, cette étude s'est appuyée sur le droit de la propriété intellectuelle et industrielle et sur le droit des affaires et en particulier le droit au « secret des affaires ». Il ressort de cette étude que l'adaptation de certaines réglementations a permis de renforcer de manière effective la protection du patrimoine informationnel dans le cadre de l'exécution d'un contrat de cloud computing. En revanche, l'adaptation de ces réglementations est vaine si elle n'est pas intégrée, dans le contrat de cloud computing, par des dispositions expresses. Le rôle de l'ingénierie

contractuelle est fondamental pour renforcer la protection des données des personnes morales dans les contrats de cloud computing. En l'occurrence, cette étude a démontré l'importance d'intégrer des clauses relatives à la sécurité technique (la sécurité de l'infrastructure cloud et la réversibilité des données) et à la sécurité juridique (la confidentialité et l'interdiction d'exploitation des données) afin d'assurer de manière effective un renforcement de la protection des données des personnes morales dans le cadre de l'exécution des contrats de cloud computing. À cette fin, il a été question de proposer de rédactions de clauses permettant de sécuriser conventionnellement les droits du client, personne morale, pour protéger son patrimoine informationnel dans le contrat de cloud computing.

# CONCLUSION GÉNÉRALE

***737. Trouver des solutions aux lacunes légales.*** Cette étude a mis en lumière l'existence de lacunes légales en matière de protection des données à caractère personnel et des données des personnes morales dans les contrats de cloud computing. Concernant la protection des données à caractère personnel, les lacunes légales résident, d'une part, dans l'absence d'une spécificité des règles de protection des données à la matière du cloud computing et d'autre part, dans l'ineffectivité des règles européennes face à la réglementation étasunienne dans le cadre d'un transfert de données. Concernant la protection des données des personnes morales, les lacunes légales résident dans l'inapplication des droits fondamentaux, de l'absence d'une réglementation spécifique à la protection des données dans le cloud et de l'absence de règles dans le cadre d'un transfert de données. Ces lacunes légales contribuent à la perte de contrôle des titulaires (personne physique et personne morale) sur leurs données et ont un impact direct dans le contrat de cloud computing pour l'établissement des droits et des obligations des parties. Pour contrer ces lacunes, des moyens juridiques et contractuels sont proposés dans la présente étude.

***738. La proposition attrayante d'une propriété des données personnelles.*** La proposition d'un droit de propriété permet d'instaurer une patrimonialité des données personnelles. Les personnes physiques seraient dotées de droits tels que le droit de rétribution pour l'utilisation des données à caractère personnel. L'admission d'un droit de rétribution des données au profit de la personne physique permettrait de rétablir un équilibre dans le marché des données. Il est proposé d'établir un cadre du marché de la donnée dans lequel l'individu serait au centre de l'autorisation de l'exploitation des données. La capacité de la personne physique de vendre et de louer les données personnelles reposerait, notamment, sur le mécanisme du *fructus* de la donnée personnelle c'est-à-dire la capacité à retirer les fruits (revenus) de l'exploitation des données réalisée par des tiers. La mise en œuvre de ce droit de rétribution est fondée sur une solution technico-juridique.

***739. Une solution technico-juridique d'un droit de rétribution des données.*** Cette autorisation d'exploitation des données pourrait se formaliser dans un contrat intelligent (smart contract) qui se fonde sur la technologie « des chaînes de blocs » qui permet d'authentifier les données et, donc, d'attester le transfert et la cession de données (sous forme d'un registre des transactions). Il a été proposé d'utiliser la chaîne de blocs comme un registre non pas des transactions des données, mais des octrois de droit d'utilisation sur ces données personnelles. Il en résulterait que c'est cet élément de preuve d'octroi de droits qui peut prendre de la valeur sous la forme d'un

actif échangé, au lieu des données elles-mêmes. Cette solution technico-juridique ne permet pas, en revanche, le stockage des données et comporte des limites liées à la non-territorialité des données et à l'identité numérique et l'identité physique.

***740. L'inadaptation du concept de propriété à la protection des données personnelles.*** Si cette proposition d'un droit de rétribution des données personnelles est attrayante sur le plan des idées (rééquilibrage des pouvoirs entre les personnes physiques et les entités), elle ne peut recevoir une application effective en raison du rejet par le droit positif français et européen d'un droit de propriété des données personnelles. En conséquence de l'inadaptation du concept de propriété, il est proposé de se tourner vers la théorie personnaliste pour renforcer la protection des données dans les contrats de cloud computing.

***741. La pertinence de la théorie personnaliste pour la protection des données personnelles.*** La théorie personnaliste est plus en phase avec les impératifs de protection des données des personnes physiques (en développant la sécurisation des données par la consécration de droits) et du marché économique (en favorisant le développement de l'innovation dans tous les domaines économiques et la compétitivité par le jeu de la libre circulation des données). Il découle de cette théorie la consécration d'un droit à l'autodétermination informationnelle. Par le droit à l'autodétermination informationnelle, il s'agit de permettre à la personne physique, dans le cadre d'un contrat de cloud computing, d'avoir un droit de contrôle sur ses données à caractère personnel ainsi que la faculté pour elle de déléguer si elle souhaite certaines prérogatives dont elle dispose sur sa donnée sans interférence de la puissance publique ou des acteurs privés. Par ailleurs, l'effectivité du droit à l'autodétermination informationnelle, pour un renforcement de la protection des données personnelles, est rendue possible par l'ingénierie contractuelle.

***742. L'ingénierie contractuelle au service de la protection des données personnelles.*** La déclinaison des droits issus du droit à l'autodétermination informationnelle est intégrée dans le contrat de cloud de computing par des dispositions spécifiques pour renforcer la protection des données personnelles. Il s'agit de prévoir dans le contrat des clauses relatives au droit de consentir à la collecte et au traitement des données, au droit d'information, au droit d'accès, au droit à la limitation du traitement, au droit d'opposition de rectification, d'effacement, au droit à la portabilité des données. Dans le cadre d'un contexte international, la protection des données est, également, renforcée par l'intégration dans le contrat cloud des clauses stipulant l'application du droit européen et l'attribution de la compétence juridictionnelle à un tribunal européen. Cette étude a produit des propositions rédactionnelles de clauses afin d'intégrer les prérogatives dans le champ contractuel et renforcer, ainsi, la protection des données personnelles.

***743. Un droit à réparation étendu.*** La protection des données personnelles est renforcée, en outre, par un droit de réparation étendu qui se traduit par un élargissement du champ de la réparation et des responsabilités. La personne physique peut obtenir une réparation de son préjudice matériel et moral en cas d'atteinte à son droit à l'autodétermination informationnelle et une réparation en l'absence même de préjudice en cas d'atteinte au droit à la vie privée. Également, elle peut exercer un recours juridictionnel contre son prestataire de services cloud ou son sous-traitant ou conjointement (responsabilité conjointe), ce qui permet à la personne concernée de renforcer son droit à obtenir une réparation effective.

***744. Le renforcement des lignes Maginot à l'international***. La portée extraterritoriale du RGPD permet de protéger les personnes situées dans l'Union européenne dont les données sont traitées, et ce indépendamment de la localisation effective du traitement. Il s'agit, donc, d'une protection élargie à toutes les personnes concernées qui se trouvent sur le territoire de l'Union européenne. En revanche, la portée extraterritoriale du règlement sur la protection des données personnelles (RGPD) a une efficacité limitée en particulier lorsque les États-Unis décident de mettre en œuvre leurs lois sécuritaires.

***745. La création d'un espace de circulation des données a-territoriale.*** Pour renforcer la protection des données dans un contexte international, il est développé l'idée de créer un espace d'échange de données déconnecté du territoire physique, lequel serait soumis aux mêmes règles de protection des données. Il pourrait s'agir, par exemple d'un espace qui aurait la taille du réseau internet. Cette proposition est une solution aux conflits de lois pouvant naître en matière de protection des données personnelles, en particulier en matière de compétence juridictionnelle. Il s'agirait de concevoir une juridiction qui serait rattachée non pas à un territoire terrestre, mais à un nouvel espace de circulation des données personnelles. L'idée d'un espace d'échange de données déconnecté du territoire apparaît dans le RGPD lorsqu'il est prévu l'application du texte indépendant de la localisation de l'activité du traitement des données. Il s'agirait, ici, de poursuivre la construction de cet espace d'échange de données en impliquant des États tiers dont les engagements seraient actés dans un accord international.

***746. L'adoption d'un accord international fondé sur le standard du RGPD.*** Face à une situation de blocage diplomatique, l'issue de sortie serait sans doute la conclusion d'accord bilatéral ou multilatéral en matière de protection des données personnelles qui encadrerait le transfert des données et réglerait la question de la compétence juridictionnelle. Il s'agirait d'adopter des conventions internationales dont le contenu reprendrait les mesures de protection des données personnelles édictées dans le RGPD. La tâche d'un consensus pourrait s'avérer ardue en raison de la grande disparité entre les systèmes juridiques des États concernant la protection des données personnelles (exemple, la Chine, les USA, et l'Union européenne).

***747. L'établissement d'un droit mondial de la protection des données personnelles.*** Indépendamment de la conclusion d'un accord international, il est aussi promu l'idée de concevoir un droit mondial de la protection des données sur le modèle de la Convention 108 du Conseil de l'Europe. En effet, un code mondial permettrait d'harmoniser les droits nationaux en matière de la protection des données personnelles, qui éviterait les situations de conflits de lois et renforcerait la protection des données personnelles au niveau mondial. Il s'agit, donc, d'une réponse à la déterritorialisation du droit. Malgré la pertinence théorique d'une telle proposition, cette solution semblerait ne pas pouvoir prospérer à l'instar de l'établissement d'une convention internationale en raison des divergences étatiques concernant, par exemple, la nature de la donnée (bien marchand ou attribut de la personnalité protégé en tant que droit fondamental).

***748. L'adaptation des réglementations à la protection du patrimoine informationnel.*** Pour renforcer la protection du patrimoine informationnel de la personne morale dans le cloud computing, il a été proposé de s'appuyer sur l'adaptation du droit de la propriété intellectuelle et industrielle et le droit des affaires. Il a été démontré des applications concrètes de protection sur certaines données de la personne morale, notamment par le droit d'auteur, le droit du producteur de la base de données, les secrets spécifiques (pour le savoir-faire et le secret de fabrique) et le secret des affaires. L'effectivité de ces droits spécifiques à la protection des données des personnes morales est réalisée par la mise en œuvre d'une ingénierie contractuelle.

***749. L'ingénierie contractuelle au service de la protection du patrimoine informationnel***. Afin de renforcer la protection du patrimoine informationnel, il a été proposé d'intégrer dans le champ contractuel des clauses relatives à ces droits spécifiques issus du droit de la propriété intellectuelle et industrielle et du droit des affaires. Cette étude a produit des propositions rédactionnelles de ces clauses afin de renforcer la protection du patrimoine informationnel. Il s'agissait de déterminer conventionnellement la mise en œuvre de ces droits afin de renforcer la protection du patrimoine informationnel dans le cadre de l'exécution d'un contrat de cloud computing. Outre l'intégration de ces droits spécifiques, l'ingénierie contractuelle consiste à proposer des clauses relatives à la sécurité technique (sécurité des données, de l'infrastructure, la réversibilité) et à la sécurité juridique (obligation d'information, de mise en garde, la confidentialité et l'interdiction de l'exploitation des données). Afin de renforcer la protection du patrimoine informationnel, il incombe, alors, au client, personne morale, de veiller à l'insertion dans le contrat de cloud computing de ces clauses dans son contrat de cloud computing.

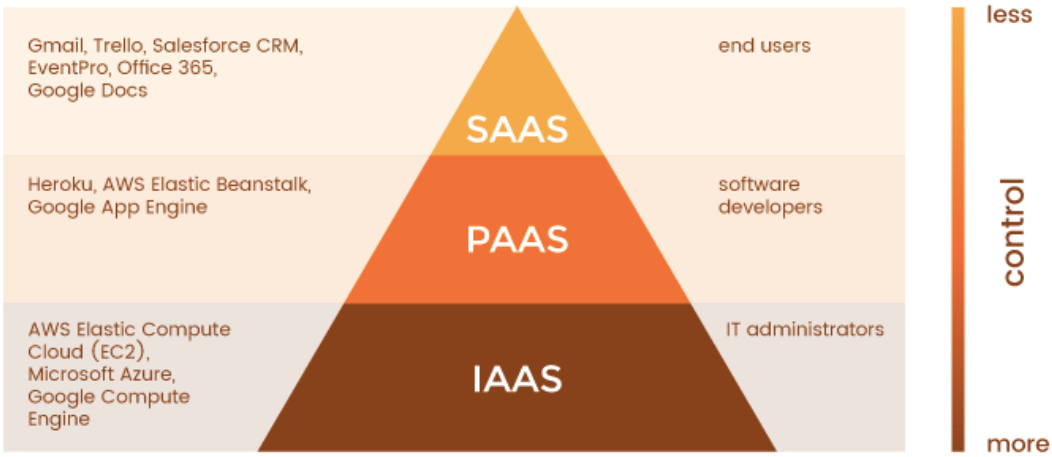
***750. Le renforcement en devenir de la protection des données des personnes morales.*** À ce jour, le régime des données des personnes morales n'est pas figé puisqu'au niveau européen des textes sont en cours d'adoption (le règlement Data Act relatif aux droits d'accès et d'utilisation des données) ou d'application (le règlement sur la gouvernance entrera en application à compter

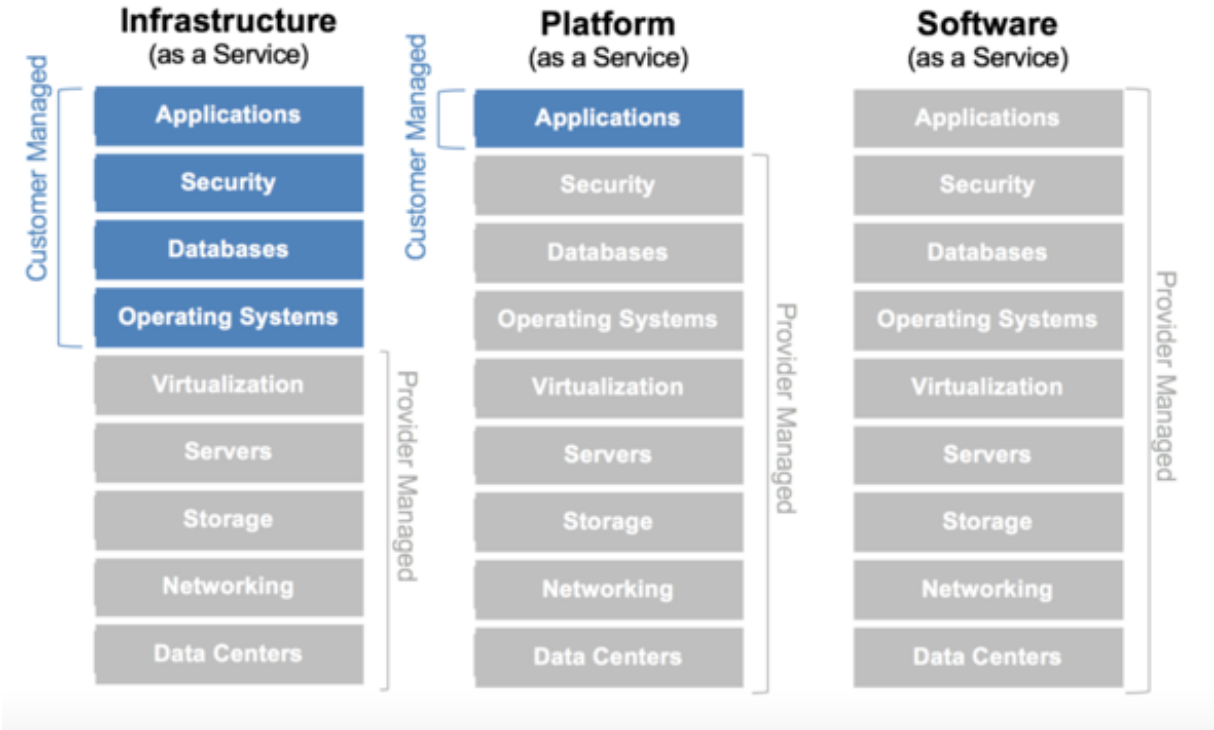
du 23 septembre 2023) afin de renforcer la protection des données des personnes morales. La protection des données des personnes morales dans le cadre d'un transfert international a été récemment renforcé par l'adoption du règlement européen sur la gouvernance des données du 30 mai 2022. Ce texte a permis de rapprocher, dans une certaine mesure, le régime des données des personnes morales à celui des personnes physiques prévu par le RGPD. Dans ce texte, il est rappelé la vision portée par la Commission qui est de créer « un marché intérieur des données dans lequel les données pourraient être utilisées quel que soit leur lieu de stockage physique dans l'Union, conformément au droit applicable, et qui soit susceptible, entre autres, de jouer un rôle déterminant dans le développement rapide des technologies de l'intelligence artificielle » (considérant 2). En définitive, il apparaît qu'en raison des enjeux économiques découlant de l'usage de la technologie du cloud computing, le législateur européen a pris conscience de la nécessité d'établir une réglementation qui puisse concilier à la fois protection des données et libre circulation des données.

# ANNEXES

# Annexe 1 : La distinction IaaS, PaaS, SaaS

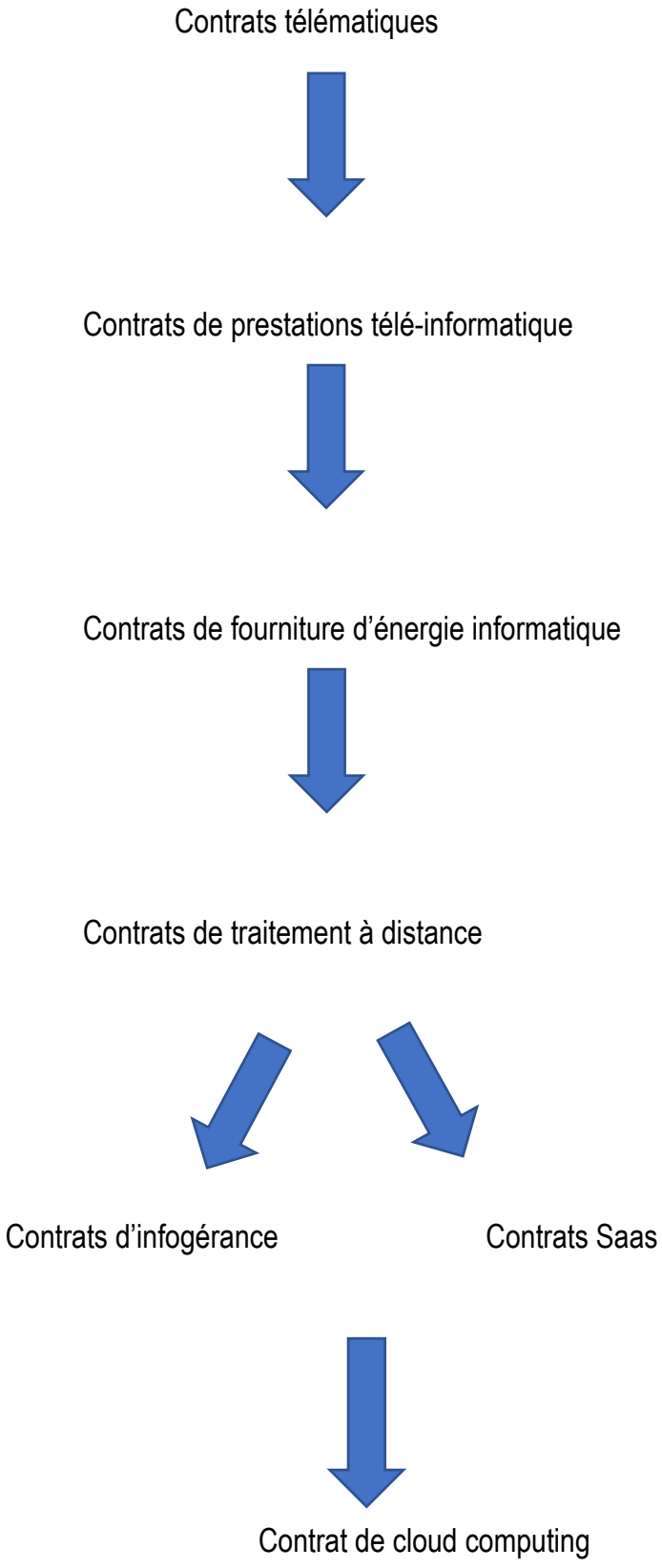
## 1) Le niveau de ressources mises à disposition



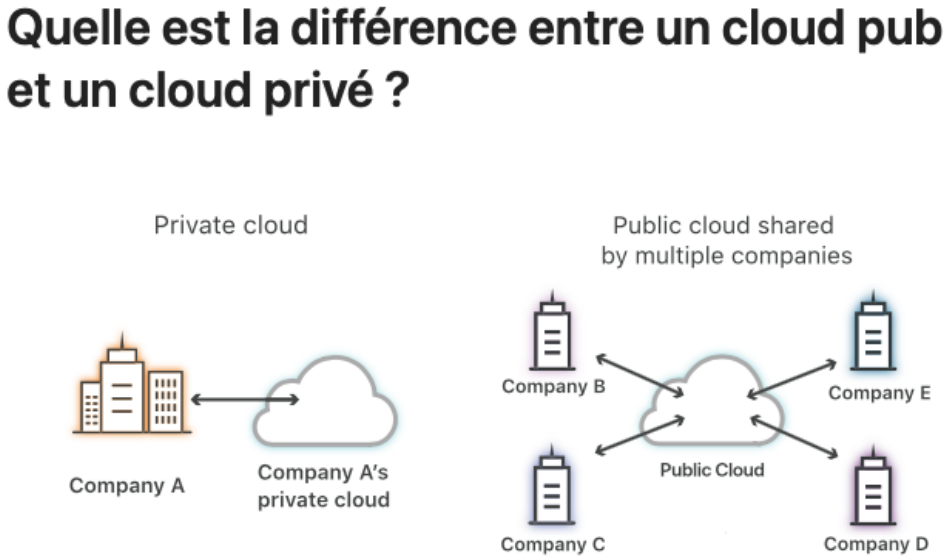




**source** : https://mbamci.com/cloud/

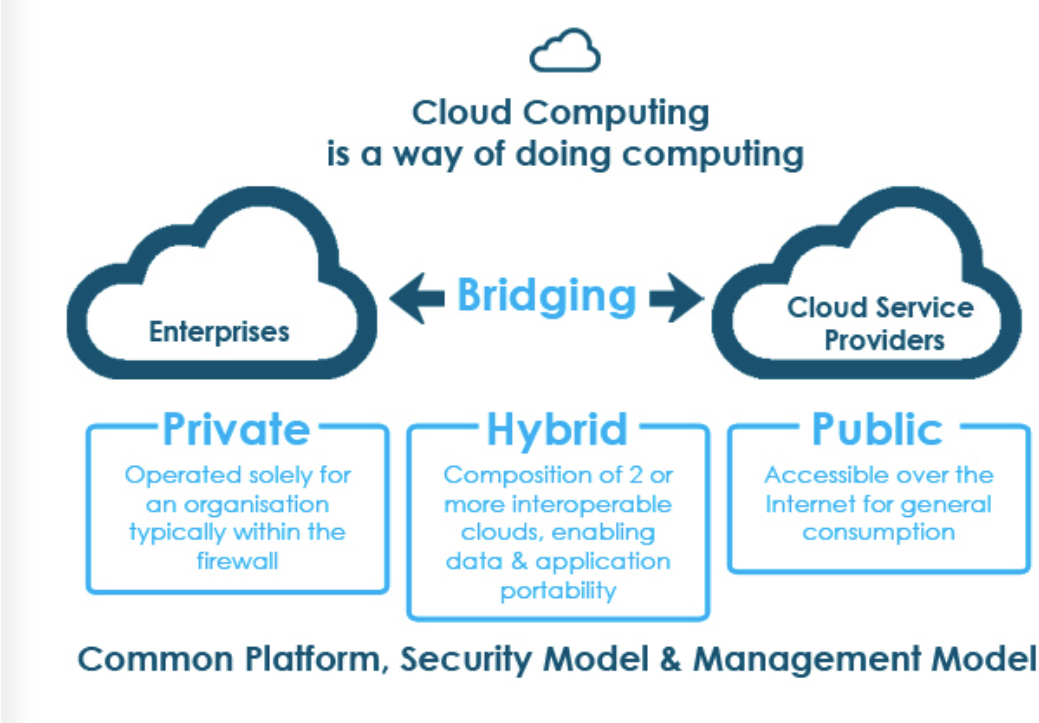
# Annexe 2 : L'illustration schématisée de la déclinaison des contrats télématiques



# Annexe 3 : La distinction des infrastructures cloud public, privé et hybride




Source : https://www.cloudflare.com/fr-fr/learning/cloud/what-is-a-public-cloud/




**source** : https://mbamci.com/cloud/.

# Annexe 4 : Clausier des principales propositions pour la protection des données des personnes physiques et des personnes morales dans le cadre d'un contrat de cloud computing

## I- En faveur de la protection des données des personnes physiques

**1) Clause relative à l'engagement de la localisation des données dans des datacenters situés sur le territoire de l'Union européenne**

Le prestataire s'engage à stocker les données du client sur des serveurs localisés dans des pays situés sur le territoire de l'Union européenne, à communiquer au Client la localisation précise des serveurs dans lesquels sont stockées les données du client, à se conformer aux directives du Client quant au choix de la localisation des serveurs pour le stockage des données, à se conformer aux obligations issues de la législation du lieu de localisation des serveurs, à informer le client de tout incident pouvant avoir sur la localisation des serveurs pour le stockage des données du client.

**2) Clause d'information générale relative aux droits de la personne physique dans le cadre d'une collecte et d'un traitement de données personnelles**

Aux fins de gestion de votre prestation de services de cloud computing, nous sommes amenés à solliciter des données personnelles vous concernant à l'occasion de la conclusion, l'exécution et la rupture de votre contrat de cloud computing. La signature du présent contrat, par vos soins, vaut autorisation pour le Prestataire de collecter, d'enregistrer et de stocker vos données personnelles lesquelles sont nécessaire pour l'exécution de votre contrat (gestion de la commande, du compte client de la relation client, de la facturation, etc..). Il vous est informé que vos données personnelles sont traitées par les services internes du Prestataire et par les partenaires du Prestataire.
Dans le cadre de l'exécution du présent contrat, Vous (client, personne physique) êtes en droit d'obtenir des informations relatives au traitement et à la collecte de vos données personnelles. Conformément au Règlement Général sur la Protection des Données (RGPD) et à la loi modifiée n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, vous pouvez demander à tout moment l'accès aux données à caractère personnel vous concernant, leur rectification, leur effacement et la limitation d'un ou plusieurs traitements particuliers de données

vous concernant, dans les conditions prévues par la Réglementation en vigueur. Vous disposez également du droit de modifier ou de retirer, à tout moment, les consentements que vous nous avez accordés pour le traitement de vos données à caractère personnel. Vous disposez par ailleurs du droit de vous opposer à un traitement de vos données à caractère personnel et du droit à leur portabilité, dans les conditions fixées par la Réglementation. Vos données à caractère personnel peuvent être conservées ou supprimées après votre décès conformément à la Réglementation. Vous disposez du droit de donner instruction au Prestataire de communiquer ces données à un tiers que vous aurez préalablement désigné. Vous pouvez exercer vos droits à tout moment en écrivant à : XXXX ou par courriel à l'adresse suivante : XXXX. Pour toute autre question concernant la collecte et le traitement de vos données personnelles, vous pouvez nous contacter par téléphone au XXXX ou par courriel à l'adresse suivante : XXXX. Nous nous engageons à répondre à vos communications dans un délai maximal de 30 (trente) jours. Pour obtenir davantage d'informations concernant la collecte et le traitement de ses données, et plus généralement la protection des données personnelles, vous avez la possibilité de consulter le document en ligne intitulé « la politique de confidentialité et de protection des données personnelles.

**3) Clause spécifique au droit d'accès de la personne physique accompagnée d'un formulaire pour l'exercice de ce droit**

Dans le cadre de l'exécution de votre contrat de cloud computing, vous disposez d'un droit d'accès aux données vous concernant conformément à la réglementation en vigueur. Ce droit d'accès vous permet d'obtenir de nos Services, la communication de vos informations personnelles ayant fait l'objet d'un traitement. Vous pouvez exercer votre droit d'accès aux données vous concernant en écrivant à : XXXX ou par courriel à l'adresse suivante : XXXX. Nous nous engageons à répondre à vos communications dans un délai maximal de 30 (trente) jours. Pour exercer votre droit d'accès, vous avez la possibilité d'utiliser le formulaire ci-dessous :

*Formulaire pour exercer le droit d'accès et à adresser à l'adresse postale suivante xxxx ou par courriel xxxx : (* informations à remplir par le client)*

Nom : *

Prénom : *

Adresse postale : *

Courriel : *

Numéro de téléphone : *

Référence du contrat : *

Madame, Monsieur,

En application de l'article 15 du Règlement général sur la protection des données (RGPD), je souhaite exercer mon droit d'accès à mes données personnelles. Je vous remercie de bien vouloir m'indiquer si des données me concernant figurent dans vos fichiers et font l'objet d'un traitement automatisé et/ou manuel. En cas de réponse positive, je demande d'obtenir la communication précise de l'ensemble de mes données personnelles faisant l'objet d'un traitement.

En application de l'article 12.3 du RGPD, je vous remercie de m'adresser la communication des informations demandées au plus tard dans un délai d'un mois à compter de la réception de ma demande. En cas de non-réponse ou de réponse incomplète, je me réserve la faculté d'adresser une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

**4) Clause spécifique au droit de rectification de la personne physique accompagnée d'un formulaire pour l'exercice de ce droit**

Dans le cadre de l'exécution de votre contrat de cloud computing, vous disposez d'un droit de rectification de vos données personnelles vous concernant conformément à la réglementation en vigueur. Ce droit de rectification vous permet d'obtenir de nos Services, la rectification de vos données personnelles ayant fait l'objet d'un traitement lorsque celles-ci sont inexactes ou incomplètes. Vous pouvez exercer votre droit de rectification de vos données vous concernant en écrivant à : XXXX ou par courriel à l'adresse suivante : XXXX. Nous nous engageons à répondre à vos communications dans un délai maximal de 30 (trente) jours. Pour exercer votre droit de rectification, vous avez la possibilité d'utiliser le formulaire ci-dessous :

*Formulaire pour exercer le droit de rectification de vos données personnelles et à adresser à l'adresse postale suivante xxxx ou par courriel xxxx : (* informations à remplir par le client)*

Nom : *

Prénom : *

Adresse postale : *

Courriel : *

Numéro de téléphone : *

Référence du contrat : *

Madame, Monsieur,

En application de l'article 16 du Règlement général sur la protection des données (RGPD), je souhaite exercer mon droit de rectification à mes données personnelles. Je vous remercie de bien vouloir rectifier les données me concernant qui sont inexactes / incomplètes *(veuillez biffer la mention inutile)* lesquelles sont détaillées ci-dessous (*veuillez indiquer précisément votre demande de rectification de vos données*) :

---

---

---.

Je vous remercie de bien vouloir me confirmer par écrit de la bonne exécution de la rectification demandée au plus tard dans un délai d'un mois à compter de la réception de ma demande. En cas de non-réponse ou de non-exécution de la rectification, je me réserve la faculté d'adresser un réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

**5) Clause spécifique au droit à la limitation du traitement de la personne physique accompagnée d'un formulaire pour l'exercice de ce droit**

Dans le cadre de l'exécution de votre contrat de cloud computing, vous disposez d'un droit à la limitation du traitement de vos données personnelles vous concernant conformément à la réglementation en vigueur. Ce droit à la limitation du traitement de vos données personnelles vous permet d'obtenir de nos Services, la limitation du traitement de vos données personnelles dans les cas prévus par la réglementation en vigueur et notamment lorsque l'exactitude des données est contestée, le traitement est illicite, les données ne sont plus nécessaires pour le responsable du traitement. Vous pouvez exercer votre droit à la limitation du traitement des données vous concernant en écrivant à : XXXX ou par courriel à l'adresse suivante : XXXX. Nous nous engageons à répondre à vos communications dans un délai maximal de 30 (trente) jours. Pour exercer votre droit à la limitation du traitement de vos données personnelles, vous avez la possibilité d'utiliser le formulaire ci-dessous :

*Formulaire pour exercer le droit à la limitation du traitement de vos données personnelles et à adresser à l'adresse postale suivante xxxx ou par courriel xxxx : (* informations à remplir par le client)*

Nom : *

Prénom : *

Adresse postale : *

Courriel : *

Numéro de téléphone : *

Référence du contrat : *

Madame, Monsieur,

En application de l'article 18 du Règlement général sur la protection des données (RGPD), je souhaite exercer mon droit de limitation du traitement de mes données personnelles.

Pour le motif suivant : (*veuillez indiquer une des raisons prévues à l'article 18 du RGPD justifiant la limitation du traitement de vos données*) ----------, je vous remercie de bien vouloir limiter le traitement de mes données concernant les informations suivantes (*veuillez indiquer précisément les données nécessitant une limitation de traitement*) :----------.

Je vous remercie de bien vouloir me confirmer par écrit de la bonne exécution de la limitation du traitement de mes données personnelles au plus tard dans un délai d'un mois à compter de la réception de ma demande. En cas de non-réponse ou de non-exécution de la limitation du traitement de mes données, je me réserve la faculté d'adresser une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

**6) Clause spécifique au droit à l'effacement des données de la personne physique accompagnée d'un formulaire pour l'exercice de ce droit**

Dans le cadre de l'exécution du contrat de cloud computing, vous disposez d'un droit à l'effacement de vos données personnelles (« droit à l'oubli ») vous concernant conformément à la réglementation en vigueur. Ce droit à l'effacement de vos données personnelles vous permet d'obtenir de nos Services, l'effacement de vos données personnelles dans tous nos fichiers électroniques et manuels. Vous pouvez exercer votre droit à l'effacement de vos données vous concernant en écrivant à : XXXX ou par courriel à l'adresse suivante : XXXX. Nous nous engageons à répondre à vos communications dans un délai maximal de 30 (trente) jours. Pour exercer votre droit à l'effacement de vos données personnelles (« droit à l'oubli »), vous avez la possibilité d'utiliser le formulaire ci-dessous :

*Formulaire pour exercer le droit à l'effacement de vos données personnelles (« droit à l'oubli ») et à adresser à l'adresse postale suivante xxxx ou par courriel xxxx : (* informations à remplir par le client)*

Nom : *

Prénom : *

Adresse postale : *

Courriel : *

Numéro de téléphone : *

Référence du contrat : *

Madame, Monsieur,

En application de l'article 17 du Règlement général sur la protection des données (RGPD), je souhaite exercer mon droit à l'effacement de mes données personnelles (« droit à l'oubli »). Je vous remercie de bien vouloir procéder à l'effacement de mes données me concernant dans tous vos fichiers électroniques et manuels.

Je vous remercie de bien vouloir me confirmer par écrit de la bonne exécution de l'effacement de mes données personnelles au plus tard dans un délai d'un mois à compter de la réception de ma demande. En cas de non-réponse ou de non-exécution de l'effacement de mes données personnelles, je me réserve la faculté d'adresser une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

**7) Clause spécifique au droit d'obtenir une notification de la personne physique accompagnée d'un formulaire pour l'exercice de ce droit**

Dans le cadre de l'exécution du contrat de cloud computing, vous disposez du droit d'obtenir une notification concernant la rectification, l'effacement, ou la limitation du traitement de vos données personnelles conformément à la réglementation en vigueur. Ce droit de notification vous permet d'obtenir de nos Services, une notification vous informant de la rectification, l'effacement, ou la limitation du traitement de vos données personnelles. Vous pouvez exercer votre droit de notification en écrivant à : XXXX ou par courriel à l'adresse suivante : XXXX. Nous nous engageons à répondre à vos communications dans un délai maximal de 30 (trente) jours. Pour exercer votre droit de notification, vous avez la possibilité d'utiliser le formulaire ci-dessous :

*Formulaire pour exercer le droit de notification et à adresser à l'adresse postale suivante xxxx ou par courriel xxxx : (* informations à remplir par le client)*

Nom : *

Prénom : *

Adresse postale : *

Courriel : *

Numéro de téléphone : *

Référence du contrat : *

Madame, Monsieur,

En application de l'article 19 du Règlement général sur la protection des données (RGPD), je souhaite exercer mon droit à obtenir une notification concernant la rectification, l'effacement, ou la limitation du traitement de vos données personnelles conformément à la réglementation en vigueur (*veuillez biffer la mention inutile*).

Je vous remercie de m'adresser la communication de la notification demandée au plus tard dans un délai d'un mois à compter de la réception de ma demande. En cas de non-réponse ou de réponse incomplète, je me réserve la faculté d'adresser une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

**8) Clause spécifique au droit d'opposition de la personne physique accompagnée d'un formulaire pour l'exercice de ce droit**

Dans le cadre de l'exécution du contrat de cloud computing, vous disposez d'un droit d'opposition concernant le traitement des données vous concernant conformément à la réglementation en vigueur. Ce droit d'opposition vous permet de vous opposer à tout moment, auprès de nos Services, à un traitement de vos données personnelles. Vous pouvez exercer votre droit d'opposition en écrivant à : XXXX ou par courriel à l'adresse suivante : XXXX. Nous nous engageons à répondre à vos communications dans un délai maximal de 30 (trente) jours. Pour exercer votre droit d'opposition au traitement des données personnelles, vous avez la possibilité d'utiliser le formulaire ci-dessous :

*Formulaire pour exercer le droit d'opposition au traitement des données personnelles et à adresser à l'adresse postale suivante xxxx ou par courriel xxxx : (* informations à remplir par le client)*

Nom : *

Prénom : *

Adresse postale : *

Courriel : *

Numéro de téléphone : *

Référence du contrat : *

Madame, Monsieur,

En application de l'article 21 du Règlement général sur la protection des données (RGPD), je souhaite exercer mon droit d'opposition au traitement de mes données personnelles. Je vous remercie de bien vouloir cesser de manière effective, à compter de la réception de ma demande, à tout traitement de mes données personnelles.

Je vous remercie de m'adresser par écrit la confirmation de la cessation du traitement de mes données personnelles au plus tard dans un délai d'un mois à compter de la réception de ma demande. En cas de non-réponse ou de non-cessation du traitement de mes données personnelles, je me réserve la faculté d'adresser une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

**9) Clause spécifique au droit à la portabilité des données de la personne physique accompagnée d'un formulaire pour l'exercice de ce droit**

Dans le cadre de l'exécution du contrat de cloud computing, vous disposez d'un droit à la portabilité des données vous concernant conformément à la réglementation en vigueur. Ce droit à la portabilité vous permet d'exiger de recevoir, de la part de nos Services, vos données personnelles dans un format adapté et structuré afin de faciliter, le cas échéant, leurs transmissions à un autre responsable du traitement des données. Vous pouvez exercer votre droit à la portabilité des vos données en écrivant à : XXXX ou par courriel à l'adresse suivante : XXXX. Nous nous engageons à répondre à vos communications dans un délai maximal de 30 (trente) jours. Pour exercer votre droit à la portabilité de vos données personnelles, vous avez la possibilité d'utiliser le formulaire ci-dessous :

*Formulaire pour exercer le droit à la portabilité de vos données personnelles et à adresser à l'adresse postale suivante xxxx ou par courriel xxxx : (* informations à remplir par le client)*

Nom : *

Prénom : *

Adresse postale : *

Courriel : *

Numéro de téléphone : *

Référence du contrat : *

Madame, Monsieur,

En application de l'article 20 du Règlement général sur la protection des données (RGPD), je souhaite exercer mon d'un droit à la portabilité de mes données personnelles. Je vous remercie de bien vouloir me fournir mes données personnelles dans un format adapté (couramment utilisé) et structuré (lisible par machine).

Le cas échéant, je vous remercie de bien vouloir transmettre ces données à caractère personnel directement à mon nouveau responsable du traitement des données, identifié ci-dessous (*veuillez biffer cette mention si elle est inutile*) :

Nom – Prénom ----------

Dénomination sociale ----------

Numéro SIRET ----------

Adresse postale ----------

Adresse électronique ----------

Numéro de téléphone ----------.

Je vous remercie de bien vouloir me transmettre mes données personnelles dans un format adapté et structuré (le cas échéant à mon responsable du traitement identifié ci-dessus), au plus tard dans un délai d'un mois à compter de la réception de ma demande. En cas de non-réponse ou de non-transmission de mes données personnelles, je me réserve la faculté d'adresser une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

# II- En faveur de la protection des données des personnes morales

**1) Clause relative à l'obligation du Prestataire de non-exploitation des œuvres du Client**

Dans le cadre des présentes, le Client n'accorde au profit du Prestataire aucune licence d'exploitation sur ses œuvres de l'esprit lesquelles sont hébergées dans l'infrastructure cloud du Prestataire. Les œuvres de l'esprit sont entendues, ici, largement et de manière non limitative comme étant celles mentionnées à l'article L.112-2 du code de la propriété intellectuelle. Le Client bénéficie d'un droit de propriété exclusif sur ses œuvres et dispose des attributs d'ordre moral (paternité, respect, divulgation, retrait et repentir concernant l'œuvre) et patrimonial (droit d'exploitation comprenant un droit de reproduction et de représentation). Le Client déclare n'accorder au Prestataire aucun droit sur ses œuvres de l'esprit. Le Prestataire reconnaît que le Client est le propriétaire exclusif de ses œuvres et qu'il ne dispose d'aucun droit sur les œuvres de son Client. Le Prestataire s'engage à ne pas utiliser, traiter, exploiter les œuvres de l'esprit hébergées dans l'infrastructure cloud sans le consentement préalable du Client. Afin de ne pas troubler la jouissance paisible du droit de propriété du Client sur ses œuvres, le Prestataire s'interdit de réaliser une quelconque action ou manipulation technique, sur les œuvres du Client, entendu largement et de manière non limitative comme : toute utilisation, toute duplication, tout traitement, toute exploitation, toute représentation, toute reproduction et toute transmission.

En cas de contravention par le Prestataire à la présente disposition ainsi qu'aux droits intellectuels et au droit de propriété du Client sur ses œuvres, le Prestataire s'engage à réparer l'intégralité des

préjudices qui résulteront de cette atteinte sans opposer une quelconque limitation de responsabilité dès lors que l'atteinte est avérée et lui est imputable.

En cas de contestation, les Parties peuvent décider, individuellement ou collectivement, de mandater un expert aux fins de constatations, de délimitation du champ de l'atteinte aux droits du Client sur ses œuvres et de déterminer l'étendue du préjudice réparable. En cas de désaccord, les Parties s'engagent, en priorité, à privilégier la résolution du litige à l'amiable avant tout recours contentieux.

**2) Clause relative à l'obligation du Prestataire de non-extraction et/ou de non-réutilisation du contenu de la base de données du Client**

Dans le cadre des présentes, le Client n'accorde au profit du Prestataire aucune licence d'exploitation du contenu de ses bases de données hébergées dans l'infrastructure cloud du Prestataire. La base de données est entendue, ici, largement et de manière non limitative comme étant « un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen » (Art. L112-3 CPI). Le Client bénéficie d'un droit de propriété exclusif sur ses bases de données et déclare n'accorder au Prestataire aucun droit sur ses bases de données. Le Prestataire reconnaît que le Client est le propriétaire exclusif de ses bases de données hébergées dans l'infrastructure cloud et qu'il ne dispose d'aucun droit sur les bases de données du Client. Le Prestataire s'engage à ne pas accéder, traiter, utiliser et exploiter les bases de données hébergées dans l'infrastructure cloud sans le consentement préalable du Client. Afin de ne pas troubler la jouissance paisible du droit de propriété de son Client sur ses bases de données, le Prestataire s'interdit de réaliser une quelconque action ou manipulation technique, sur les bases de données de son Client, entendu largement et de façon non limitative comme : tout traitement, toute exploitation, toute représentation, toute reproduction, toute extraction et/ou réutilisation totale ou partielle d'une partie substantielle ou non de la base de données.

En cas de contravention par le Prestataire à la présente disposition ainsi qu'aux droits intellectuels et au droit de propriété du Client sur ses bases de données, le Prestataire s'engage à réparer l'intégralité des préjudices qui résulteront de cette atteinte sans opposer une quelconque limitation de responsabilité dès lors que l'atteinte est avérée et lui est imputable.

En cas de contestation, les Parties peuvent décider, individuellement ou collectivement, de mandater un expert aux fins de constatations, de délimitation du champ de l'atteinte aux droits du Client sur ses bases de données et de déterminer l'étendue du préjudice réparable. En cas de désaccord, les Parties s'engagent, en priorité, à privilégier la résolution du litige à l'amiable avant tout recours contentieux.

**3) Clause relative à l'obligation du Prestataire de non-accès, de non-traitement et de non-exploitation des données relatives au savoir-faire du Client**

Dans le cadre des présentes, le Client n'accorde au profit du Prestataire aucune licence d'exploitation de son savoir-faire hébergé dans l'infrastructure cloud du Prestataire. Le savoir-faire du Client est entendu, ici, largement et de manière non limitative comme étant « un ensemble d'informations pratiques non breveté, résultant de l'expérience et testé, qui est secret, substantiel et identifié » (art. 1er du règlement d'exemption n° 772/2004 du 27 avril 2004). Il est entendu que les informations couvertes par le savoir-faire (ci-après désignées « Savoir-faire ») sont protégées par les présentes et incluent de manière non limitative, toute information non brevetée sous support électronique relative à toute documentation, toute spécification ou tout procédé commercial, technique (fabrication, informatique …), marketing, financier et à tout projet de recherche de développement présent ou futur du Client. Le Client bénéficie d'un droit de propriété exclusif sur son savoir-faire et déclare n'accorder au Prestataire aucun droit sur son savoir-faire. Le Prestataire reconnaît que le Client est le propriétaire exclusif de son savoir-faire et qu'il ne dispose d'aucun droit sur le savoir-faire du Client. Le Prestataire s'engage à ne pas contrevenir à la confidentialité du savoir -faire et à ne pas accéder, traiter ou utiliser le savoir-faire hébergé dans l'infrastructure cloud sans le consentement préalable du Client. Afin de ne pas troubler la jouissance paisible du droit de propriété du Client sur son savoir-faire, le Prestataire s'interdit de réaliser une quelconque action ou manipulation technique, sur le savoir-faire du client, entendu largement et de manière non limitative comme : tout accès, toute utilisation, toute duplication, tout traitement, toute exploitation, toute représentation, toute reproduction, toute transmission.

En cas de contravention par le Prestataire à la présente disposition ainsi qu'aux droits intellectuel et de propriété du Client sur son savoir-faire, le Prestataire s'engage à réparer l'intégralité des préjudices qui résulteront de cette atteinte sans opposer une quelconque limitation de responsabilité dès lors que l'atteinte est avérée et lui est imputable.

En cas de contestation, les Parties peuvent décider, individuellement ou collectivement, de mandater un expert aux fins de constatations, de délimitation du champ de l'atteinte aux droits du Client sur son savoir-faire et de détermination de l'étendue du préjudice réparable. En cas de désaccord, les Parties s'engagent, en priorité, à privilégier la résolution du litige à l'amiable avant tout recours contentieux.

**4) Clause relative à l'obligation du Prestataire de non-accès, de non-traitement et de non-exploitation des données relatives au secret de fabrique du Client**

Dans le cadre des présentes, le Client n'accorde au profit du Prestataire aucune licence d'exploitation sur ses données, et en particulier, les données relatives au secret de fabrique (ci-après désignées « secret de fabrique ») hébergées dans l'infrastructure cloud du Prestataire. Il est entendu que les informations couvertes par le secret de fabrique sont protégées par les présentes et incluent de manière non limitative, toute information non brevetée sous support électronique, toute documentation, toute spécification d'un procédé de fabrication et/ou des caractéristiques techniques ayant pour objet la fabrication. Le Client bénéficie d'un droit de propriété exclusif sur son secret de fabrique et déclare n'accorder au Prestataire aucun droit sur les données couvertes par le secret de fabrique. Le Prestataire reconnaît que le Client est le propriétaire exclusif de son secret de fabrique et qu'il ne dispose d'aucun droit sur le secret de fabrique du Client. Le Prestataire s'engage à ne pas contrevenir à la confidentialité du secret de fabrique et à ne pas accéder, traiter ou utiliser le secret de fabrique hébergé dans l'infrastructure cloud sans le consentement préalable du Client. Afin de ne pas troubler la jouissance paisible du droit de propriété du Client sur son secret de fabrique, le Prestataire s'interdit de réaliser une quelconque action ou manipulation technique, sur le secret de fabrique, entendu largement et de manière non limitative comme : tout accès, toute utilisation, toute duplication, tout traitement, toute exploitation, toute représentation, toute reproduction, toute transmission.

En cas de contravention par le Prestataire à la présente disposition ainsi qu'aux droits intellectuels et de propriété du Client sur son secret de fabrique, le Prestataire s'engage à réparer l'intégralité des préjudices qui résulteront de cette atteinte sans opposer une quelconque limitation de responsabilité dès lors que l'atteinte est avérée et lui est imputable.

En cas de contestation, les Parties peuvent décider, individuellement ou collectivement, de mandater un expert aux fins de constatations, de délimitation du champ de l'atteinte aux droits du Client sur son secret de fabrique et de détermination de l'étendue du préjudice réparable. En cas de désaccord, les Parties s'engagent, en priorité, à privilégier la résolution du litige à l'amiable avant tout recours contentieux.

**5) Clause relative à l'obligation de confidentialité du Prestataire**

Le Prestataire s'engage à ne communiquer les données confidentielles appartenant au client à aucune personne ou entité et à prendre toutes mesures nécessaires pour éviter que son personnel ne divulgue à des tiers tout ou partie desdites données. Le Prestataire s'engage à ne pas entreprendre d'actions directes ou indirectes susceptibles de mettre en péril la confidentialité des données

stockées dans le cloud. Également, le Prestataire s'engage à garantir la confidentialité des données du client en mettant en œuvre tous les moyens techniques nécessaires pour sécuriser le cloud contre toute ingérence ou intrusion de tiers non autorisés. En cas de contravention, aux présentes dispositions, le Prestataire engage sa responsabilité avec pour sanction le paiement au profit du Client d'une indemnisation compensatrice d'un montant équivalent à X % du montant du préjudice évalué. Étant précisé qu'en cas de désaccord sur l'évaluation du montant du préjudice, il sera possible pour l'une ou l'autre des parties au contrat de faire appel à une expertise. En cas de contravention par le Prestataire à l'une des obligations du présent article, le Client dispose, également, de la faculté de résilier le présent contrat à la charge du Prestataire.

**6) Accord de confidentialité des données de la personne morale (annexe au contrat de cloud computing)**

**ACCORD DE CONFIDENTIALITÉ DES DONNÉES HÉBERGÉES DANS LE CLOUD**

**ANNEXE AU CONTRAT DE CLOUD COMPUTING**

entre

**.....,** société ..... *(forme de la société)*, ayant son siège social ..... *(adresse du siège social)*, enregistrée au Registre du Commerce et des Sociétés de ..... *(localité du RCS),* sous le numéro ..... *(n° RCS)*, représentée par M. / Mme..... (nom du représentant), ..... *(qualité du représentant),* dûment habilité à l'effet des présentes,

ci-après désigné(e) par **« le Prestataire »,**

**D'UNE PART,**

**ET**

**.....,** société ..... *(forme de la société)*, ayant son siège social ..... *(adresse du siège social)*, enregistrée au Registre du Commerce et des Sociétés de ..... *(localité du RCS),* sous le numéro ..... *(n° RCS)*, représentée par M. / Mme ..... (nom du représentant), ..... *(qualité du représentant),* dûment habilité à l'effet des présentes,

ci-après désigné(e) par **« le Client »,**

**D'AUTRE PART,**

**PRÉAMBULE**

Dans le cadre de la conclusion d'un contrat de cloud computing, les Parties acceptent d'annexer au contrat de cloud computing (ci-après désigné contrat principal), le présent accord relatif à la confidentialité des données hébergées dans l'infrastructure en nuage.

Afin de protéger l'ensemble des informations confidentielles du Client hébergées dans l'infrastructure en nuage du Prestataire, les Parties ont l'intention de s'engager juridiquement et sont convenues de ce qui suit :

**Article 1 - Définitions**

**1.1 1.1** Le terme « DONNÉES CONFIDENTIELLES », désigne les informations de toute nature détenues par le Client incluant de manière non limitative : le savoir -faire, le secret de fabrique, les informations de nature commerciale (étude de marché, portefeuille client et fournisseur de l'entreprise…), financière (informations sur le chiffre d'affaires, bénéfices, pertes ), contractuelle (conditions particulières accordées telles que les prix, ristournes, quantités achetées, date d'expiration de garanties...), marketing (stratégies de communication et de développement, procédés et outils marketing utilisés), technique (procédés techniques de développement des produits, logiciel, code-source..) et plus généralement, toute documentation sous format électronique s'y rapportant. En particulier, sont confidentielles les informations ayant une valeur économique réelle ou potentielle ou un avantage concurrentiel certain propre dont le public ou toute autre personne, y compris le Prestataire, pourrait retirer de leur divulgation ou utilisation une valeur économique ou un avantage concurrentiel.

Ces DONNÉES CONFIDENTIELLES constituent l'objet du présent accord et seront avec le présent Engagement tenus pour confidentiels.

**Article 2 – Objet**

L'accord a pour objet de fixer les règles relatives à la protection des DONNÉES CONFIDENTIELLES appartenant exclusivement au Client et qui sont hébergées dans l'infrastructure en nuage du Prestataire.

Le présent accord couvre, également, l'ensemble des discussions relatives au contrat principal et la période de discussion, de négociation et d'exécution dudit contrat.

**Article 3 – Déclarations du Client**

Le Client déclare qu'il bénéficie d'un droit de propriété exclusif sur ses DONNÉES CONFIDENTIELLES et n'accorder, au Prestataire, aucun droit sur lesdites données.

**Article 4 - Obligations du Prestataire**

**4.1** Le prestataire s'engage à garantir la confidentialité des DONNÉES CONFIDENTIELLES du client en mettant en œuvre tous les moyens techniques nécessaires pour sécuriser le cloud contre toute ingérence ou intrusion de tiers non autorisés.

**4.2** Le Prestataire s'engage à ne communiquer les DONNÉES CONFIDENTIELLES appartenant au Client à aucune personne ou entité et à prendre toutes mesures nécessaires pour éviter que son personnel ne divulgue à des tiers tout ou partie desdites données.

**4.3** Le Prestataire s'engage à ne pas entreprendre d'actions directes ou indirectes susceptibles de mettre en péril la confidentialité des données hébergées dans le cloud, objet du contrat, sous peine de voir sa responsabilité engagée conformément à l'article 7 du présent accord.

**4.4** Le Prestataire s'engage à ne pas accéder, à utiliser, traiter, exploiter les DONNÉES CONFIDENTIELLES sans une autorisation préalable du Client.

**4.5** Le Prestataire s'engage à ne pas troubler la jouissance paisible du droit de propriété du Client sur ses DONNÉES CONFIDENTIELLES et s'interdit de réaliser une quelconque action ou manipulation technique sur lesdites données de son Client, entendu largement et de manière non limitative comme : toute utilisation, toute duplication, tout traitement, toute exploitation, toute représentation, toute reproduction et toute transmission.

**4.6** S'agissant de l'utilisation de certaines données prévue à l'article 6 du présent accord, le Prestataire s'engage à ne procéder à aucune duplication, sous quelque forme et quelque support que ce soit, de tout ou partie de l'information transmise, sans l'autorisation écrite et préalable du Client.

**4.7** Dans les trente (30) jours suivant l'expiration du contrat de cloud computing, le Prestataire s'engage à restituer ou à détruire l'intégralité des DONNÉES CONFIDENTIELLES en sa possession et certifier par écrit ne pas avoir conservé de DONNÉES CONFIDENTIELLES et/ou de reproductions, sur quelque support que ce soit.

**Article 5 – Propriété des données**

**5.1** Le Client demeure le propriétaire exclusif de ses DONNÉES CONFIDENTIELLES qui sont hébergées dans les serveurs de l'infrastructure en nuage du Prestataire.

**5.2** Le présent Accord n'autorise aucun transfert de propriété sur ses DONNÉES CONFIDENTIELLES au profit du Prestataire.

**5.3** Le présent Accord ne peut, en aucun cas, être interprété comme conférant de manière implicite une concession de licence de brevet, de marque ou d'autres droits de propriété intellectuelle ou industrielle reconnus par la loi.

**Article 6 – Utilisation autorisée de certaines DONNÉES CONFIDENTIELLES**

Le Prestataire ayant connaissance d'une DONNÉE CONFIDENTIELLE s'engage à ne l'utiliser que dans le cadre du présent Contrat et pour les seuls besoins pour lesquels cette information est communiquée et reconnaît que cette information reste, en tout état de cause, la propriété du Client.

**Article 7 - Responsabilité et clause pénale**

En cas de contravention à l'une des dispositions du présent Accord et plus généralement d'une atteinte à la protection des DONNÉES CONFIDENTIELLES, le Prestataire s'engage à réparer l'intégralité des préjudices qui résulteront de cette atteinte sans opposer une quelconque limitation de responsabilité dès lors que l'atteinte est avérée et lui est imputable. À ce titre, le Prestataire s'engage à verser au profit du Client une indemnisation compensatrice d'un montant équivalent à X % du montant du préjudice évalué. En cas de désaccord sur l'évaluation du montant du préjudice, il est possible pour l'une ou l'autre des parties de faire appel à une expertise conformément à l'article 10 du présent accord.

**Article 8 – Durée**

L'Accord entre en vigueur à compter de la date de signature du contrat principal par les Parties et est conclu pour la durée de validité du contrat principal.

**Article 9 – Résiliation**

L'accord ne peut être résilié indépendamment de la résiliation du contrat principal signé entre les Parties.

**Article 10 – Litiges et droit applicable.**

**9.1** Le présent accord est soumis à la réglementation française en vigueur.

**9.2** En cas de contestation, les Parties peuvent décider, individuellement ou collectivement, de mandater un expert aux fins de constatations, de délimitation du champ de l'atteinte aux droits du Client sur ses DONNÉES CONFIDENTIELLES et de détermination de l'étendue du préjudice réparable.

**9.3** En cas de désaccord, les Parties s'engagent, en priorité, à privilégier la résolution du litige à l'amiable avant tout recours contentieux.

**9.4** En cas de contestation persistante, les Parties acceptent de soumettre leur différend aux juridictions françaises compétentes.

Fait le ..... *(date),* A ..... *(lieu),*

En deux exemplaires originaux,

Pour le Prestataire (signature)

Pour le Client (signature)

**7) Accord de protection du secret des affaires (annexe au contrat de cloud computing)**

## ACCORD DE PROTECTION DES DONNÉES DU SECRET D'AFFAIRES

### ANNEXE AU CONTRAT DE CLOUD COMPUTING

entre

**.....,** société ..... *(forme de la société)*, ayant son siège social ..... *(adresse du siège social)*, enregistrée au Registre du Commerce et des Sociétés de ..... *(localité du RCS),* sous le numéro ..... *(n° RCS)*, représentée par M. / Mme..... (nom du représentant), ..... *(qualité du représentant),* dûment habilité à l'effet des présentes,

ci-après désigné(e) par **« le Prestataire »,**

**D'UNE PART,**

**ET**

**.....,** société ..... *(forme de la société)*, ayant son siège social ..... *(adresse du siège social)*, enregistrée au Registre du Commerce et des Sociétés de

..... *(localité du RCS),* sous le numéro ..... *(n° RCS)*, représentée par M. / Mme ..... (nom du représentant), ..... *(qualité du représentant),* dûment habilité à l'effet des présentes,

ci-après désigné(e) par **« le Client »,**

**D'AUTRE PART,**

**PRÉAMBULE**

Dans le cadre de la conclusion d'un contrat de cloud computing, les Parties acceptent d'annexer au contrat de cloud computing (ci-après désigné contrat principal), le présent accord relatif à la protection des données du secret d'affaires.

Afin de protéger les informations confidentielles du Client couvertes par le secret des affaires, les Parties ont l'intention de s'engager juridiquement et sont convenues de ce qui suit :

**Article 1 - Définitions**

**1.1** Le terme « DONNÉE(S) », désigne les informations de toute nature détenues par le Client incluant de manière non limitative : le savoir -faire, le secret de fabrique, les informations de nature commerciale (étude de marché, portefeuille client et fournisseur de l'entreprise…), financière (informations sur le chiffre d'affaires, bénéfices, pertes ), contractuelle (conditions particulières accordées telles que les prix, ristournes, quantités achetées, date d'expiration de garanties...), marketing (stratégies de communication et de développement, procédés et outils marketing utilisés), technique (procédés techniques de développement des produits, logiciel, code-source..) et plus généralement, toute documentation sous format électronique s'y rapportant.

**1.2** Le terme « Secret d'affaires » désigne la protection offerte par la loi concernant les DONNÉES confidentielles des personnes morales ayant une valeur économique et faisant l'objet de mesures de protection destinées à les garder secrètes.

Ces DONNÉES constituent l'objet du présent accord et seront ainsi tenues pour confidentielles.

**Article 2 – Objet**

L'accord a pour objet de fixer les règles relatives à la protection de la DONNÉE du Client hébergée dans l'infrastructure en nuage du Prestataire.

**Article 3 – Déclarations du Client**

Le Client déclare qu'il bénéficie d'un droit de propriété exclusif sur sa DONNÉE et n'accorder, au Prestataire, aucun droit sur sa DONNÉE.

**Article 4 - Obligations du Prestataire**

**4.1** Le Prestataire s'engage à ne pas accéder, à utiliser, traiter, exploiter la DONNÉE, appartenant exclusivement au Client, hébergée dans les serveurs de son infrastructure en nuage.

**4.2** Le Prestataire s'engage à ne pas troubler la jouissance paisible du droit de propriété du Client sur sa DONNÉE et s'interdit de réaliser une quelconque action ou manipulation technique sur la DONNÉE de son

Client, entendu largement et de manière non limitative comme : toute utilisation, toute duplication, tout traitement, toute exploitation, toute représentation, toute reproduction et toute transmission.

**4.3** Le Prestataire s'engage à ne communiquer la DONNÉE appartenant au Client à aucune personne ou entité et à prendre toutes mesures nécessaires pour éviter que son personnel ne divulgue à des tiers tout ou partie de la DONNÉE.

**Article 5 – Propriété des données**

**5.1** Le Client demeure le propriétaire exclusif de la DONNÉE hébergée dans les serveurs de l'infrastructure en nuage du Prestataire.

**5.2** Le présent Accord n'autorise aucun transfert de propriété´ au profit du Prestataire.

**5.3** Le présent Accord ne peut, en aucun cas, être interprété comme conférant de manière implicite une concession de licence de brevet, de marque ou d'autres droits de propriété intellectuelle ou industrielle reconnus par la loi.

**Article 6 – Responsabilité**

En cas de contravention à l'une des dispositions du présent Accord et plus généralement d'une atteinte à la protection des DONNÉES du secret d'affaires, le Prestataire s'engage à réparer l'intégralité des préjudices qui résulteront de cette atteinte sans opposer une quelconque limitation de responsabilité dès lors que l'atteinte est avérée et lui est imputable.

**Article 6 – Durée**

L'Accord entre en vigueur à compter de la date de signature du contrat principal par les Parties et est conclu pour la durée de validité du contrat principal.

**Article 7 – Résiliation**

L'accord ne peut être résilié indépendamment de la résiliation du contrat principal signé entre les Parties.

**Article 9 – Litiges et droit applicable.**

**9.1** Le présent accord est soumis à la réglementation française en vigueur.

**9.2** En cas de contestation, les Parties peuvent décider, individuellement ou collectivement, de mandater un expert aux fins de constatations, de délimitation du champ de l'atteinte aux droits du Client sur sa DONNÉE et de détermination de l'étendue du préjudice réparable.

**9.3** En cas de désaccord, les Parties s'engagent, en priorité, à privilégier la résolution du litige à l'amiable avant tout recours contentieux.

**9.4** En cas de contestation persistante, les Parties acceptent de soumettre leur différend aux juridictions françaises compétentes.

Fait le ..... *(date),* A ..... *(lieu),*

En deux exemplaires originaux,

Pour le Prestataire (signature)

Pour le Client (signature)

**8) Clause relative à l'obligation générale de conseil, d'information et de mise en garde du Prestataire**

Le Prestataire, préalablement à la conclusion du contrat, s'engage à communiquer au Client toutes les informations utiles et pertinentes concernant la prestation de services choisie par le Client. Il s'engage à remettre au client, avant la conclusion du contrat, la documentation technique et précontractuelle attachée à ladite prestation de services et à rester à la disposition du Client pour répondre aux éventuelles interrogations. Le Prestataire met en garde le Client de s'entourer de tous les conseils nécessaires à la contractualisation d'une offre de services cloud et en particulier concernant le choix des modules de services cloud. Le Prestataire informe le Client qu'il lui incombe de s'assurer de la pertinence et de l'adaptation de la prestation de services choisie par rapport à ses besoins et ses attentes. Le Prestataire informe le Client qu'il ne pourra pas être tenu pour responsable en cas d'erreur par le Client concernant le choix de la prestation de services ou leurs adaptations par rapport à ses besoins.

**9) Clause relative à l'obligation spécifique d'information du Prestataire concernant la localisation des données**

Le Prestataire informe le Client que ses données sont hébergées dans des serveurs appartenant au Prestataire lesquels sont situés sur le territoire de l'Union européenne. Le prestataire s'engage à se conformer à la localisation des données choisie par le client lors de la souscription aux services cloud. Sauf accord contraire des Parties, le prestataire s'engage à ne transférer ni héberger aucune des données du Client dans des serveurs situés hors de l'Union européenne. Le Prestataire s'engage à informer, sans délai, le client lorsque les données sont transférées, pour un motif légitime (notamment en application d'une réglementation impérative ou une décision juridictionnelle ayant force obligatoire), dans un centre de données situé en dehors de la localisation choisie par le client.

**10) Clause relative à l'obligation du Prestataire de non-exploitation des données du Client**

Dans le cadre des présentes, le Client n'accorde au profit du Prestataire aucune licence d'exploitation de ses données lesquelles sont hébergées dans l'infrastructure en nuage du

Prestataire. Les données sont entendues, ici, largement comme étant les informations de toute nature détenues par le Client incluant de manière non limitative : le savoir -faire, le secret de fabrique, les informations de nature commerciale (étude de marché, portefeuille client et fournisseur de l'entreprise…), financière (informations sur le chiffre d'affaires, bénéfices, pertes ), contractuelle (conditions particulières accordées telles que les prix, ristournes, quantités achetées, date d'expiration de garanties...), marketing (stratégies de communication et de développement, procédés et outils marketing utilisés), technique (procédés techniques de développement des produits, logiciel, code-source..) et plus généralement, toute documentation sous format électronique s'y rapportant. Le Client bénéficie d'un droit de propriété exclusif sur les données hébergées dans l'infrastructure du nuage du Prestataire. Le Prestataire s'engage à ne pas utiliser, traiter, exploiter les données hébergées dans l'infrastructure cloud sans le consentement préalable du Client. Également, le Prestataire s'interdit de réaliser une quelconque action ou manipulation technique sur lesdites données, entendu largement et de manière non limitative comme : toute utilisation, toute duplication, tout traitement, toute exploitation, toute représentation, toute reproduction et toute transmission.

En cas de contravention à la présente disposition, le Prestataire s'engage à réparer l'intégralité des préjudices qui résulteront de cette atteinte sans opposer une quelconque limitation de responsabilité dès lors que l'atteinte est avérée et lui est imputable. Le Prestataire sera redevable au profit du Client du paiement d'une indemnisation compensatrice d'un montant équivalent à xx % du montant du préjudice évalué. Le Client disposera de la faculté de résilier le contrat de cloud computing aux torts exclusifs du Prestataire.

En cas de contestation, les Parties peuvent décider, individuellement ou collectivement, de mandater un expert aux fins de constatations, de délimitation du champ de l'atteinte aux droits du Client sur ses œuvres et de déterminer l'étendue du préjudice réparable. En cas de désaccord, les Parties s'engagent, en priorité, à privilégier la résolution du litige à l'amiable avant tout recours contentieux.

**11) Clause relative à l'obligation du Client de sécuriser l'accès aux données hébergées dans le cloud**

Pour assurer la sécurité des données hébergées dans le cloud computing, il est mis à la charge du Client une obligation de sécuriser l'accès à ces données hébergées dans le cloud computing. Il incombe au Client de prendre toutes les mesures nécessaires et appropriées pour sécuriser ses données, telles qu'un accès restreint à certaines personnes et l'établissement de mots de passe pour accéder au serveur. En cas de négligence avérée par le Client concernant son obligation de sécuriser les données, le prestataire ne sera pas tenu pour responsable.

**12) Clause relative à l'obligation du Prestataire de sécuriser l'infrastructure cloud**

Pendant toute la durée du contrat, le prestataire s'engage à assurer la sécurité de ses infrastructures en nuage. Le Prestataire informe le Client que les serveurs hébergeant ces données disposent d'une sécurité d'accès et d'un accès physique restreint et sélectif du bâtiment. À ce titre, le prestataire s'engage à mettre en œuvre des mesures de sécurité technique et organisationnelle pour assurer la sécurité de l'infrastructure cloud, telle que des mesures de chiffrement, des mesures permettant d'assurer la confidentialité, l'intégrité, la disponibilité et la résilience permanentes des systèmes et services de traitement, des mesures d'identification et d'autorisation des utilisateurs, des mesures de protection des données lors de la transmission, les mesures de protection pendant le stockage. Est annexé au présent contre, un document technique qui énumère les mesures techniques mises en œuvre par le Prestataire pour assurer la sécurité de l'infrastructure cloud.

**13) Clause relative à l'engagement de la responsabilité du Prestataire applicable dans le cadre de la sous-traitance**

Le Prestataire est responsable de plein droit à l'égard du Client de la bonne exécution des obligations résultant du contrat et de ses annexes, que ces obligations soient à exécuter par lui-même ou par son (ses) sous-traitant(s). Le prestataire de service cloud s'engage à se conformer aux obligations stipulées dans le contrat et ses annexes et à s'assurer du respect de ces obligations lorsqu'une partie ou l'intégralité de la prestation, objet du contrat, est confiée à un tiers au contrat. En cas de contravention à l'une des obligations prévues au contrat et ses annexes par lui-même et/ou son (ses) sous-traitant(s), le Prestataire s'engage à réparer l'intégralité des préjudices subis par le Client qui résulteront de cette atteinte sans opposer une quelconque limitation de responsabilité. À ce titre, le prestataire s'engage à verser au profit du Client une indemnisation compensatrice d'un montant équivalent à X % du montant du préjudice évalué. En cas de désaccord sur l'évaluation du montant du préjudice, il est possible pour l'une ou l'autre des parties de faire appel à une expertise. Le Prestataire peut s'exonérer de tout ou partie de sa responsabilité en apportant la preuve que l'inexécution ou la mauvaise exécution du contrat est imputable soit au Client, soit au fait, imprévisible et insurmontable, d'un tiers étranger (hormis son (ses) sous-traitant(s)) à la fourniture des prestations prévues au contrat, soit à un cas de force majeure.

**14) Clause relative au droit applicable et à la compétence juridictionnelle**

Le présent accord ainsi que ses annexes sont soumis à la réglementation française en vigueur.

En cas de différend entre le Prestataire et le Client professionnel, la compétence juridictionnelle est attribuée expressément aux tribunaux français territorialement et matériellement compétents, nonobstant pluralité de défendeurs ou appel en garantie, y compris pour les mesures d'urgence, conservatoires en référé ou sur requête.

# RÉSUMÉ DE THÈSE EN FRANÇAIS

**Titre** : La protection des données dans les contrats de cloud computing.

Le sujet envisagé de cette thèse est relatif à la protection des données à caractère personnel des personnes physiques et des personnes morales de droit privé dans les contrats de cloud computing. L'accélération de la technologie numérique et le développement des services de cloud computing ont contribué à porter atteinte aux données. Par ce constat, le droit est intervenu et tente toujours d'apporter des solutions juridiques à ce besoin de protection des données numériques. L'intérêt de cette étude réside dans le constat que la technologie du cloud computing suscite des interrogations juridiques en ce qui concerne l'effectivité du droit et de la responsabilité des acteurs du cloud computing. Ces interrogations s'amplifient par l'effet de la mondialisation et du principe de libre circulation des données promu à l'échelle européenne. Dans ce contexte, la question est de savoir comment renforcer la protection des données dans les contrats de cloud computing ?

La réflexion sur le renforcement de la protection des données est menée à partir d'un triptyque de protection attendue, la protection technologique, la protection légale et la protection contractuelle. Les travaux de recherches sont basés sur l'étude des mesures techniques de protection des données, du cadre légal (national, européen et étasunien) applicable à la protection des données et sur l'analyse des contrats de cloud computing.

Cette étude a été réalisée en vue d'apporter des solutions aux lacunes légales et aux insuffisances technologiques pour protéger les données des personnes physiques et des personnes morales dans le cadre de l'exécution d'un contrat de cloud computing. Les solutions proposées reposent essentiellement sur l'adaptation du droit à la protection des données à caractère personnel des personnes physiques et du patrimoine informationnel des personnes morales, et l'ingénierie contractuelle.

# SUMMARY OF THE THESIS IN ENGLISH

**Title:** Data protection in cloud computing contracts.

The subject of this thesis is related to the data protection of individuals and legal entities in cloud computing contracts.

The acceleration of digital technology and the development of cloud computing services have contributed to the infringement of data protection rights. The law has therefore intervened and is still trying to provide legal solutions to this need for digital data protection. The interest of carrying out a thesis on data protection in cloud computing contracts lies in the fact that cloud computing technology raises legal questions, in particular the question of the effectiveness of the law and the responsibility of cloud computing actors. These questions are amplified by the effect of globalization and the principle of free circulation of data promoted at the European level. In this context, the issue is how to reinforce data protection in cloud computing contracts? The reflection is conducted from a triptych of expected protection, technological protection, legal protection, and contractual protection. The research is based on the study of technical data protection measures, the legal framework (national, European, and American) applicable to data protection and the analysis of cloud computing contracts.

This thesis was conducted to provide solutions to the legal gaps and technological shortcomings to protect the data of individuals and legal entities in the context of the execution of a cloud computing contract. The proposed solutions are essentially based on the adaptation of the law to the protection of the personal data of individuals and the information assets of legal entities, and on contractual engineering.

# BIBLIOGRAPHIE

## I. OUVRAGES JURIDIQUES GENERAUX : TRAITES, MANUELS, PRECIS ET DICTIONNAIRES


**Azéma J. et Galloux J.-C.**

- *Droit de la propriété industrielle*, Dalloz, coll. *Précis*, 8e éd., 2017.

**Bénabent A.**

- *Droit des contrats spéciaux civils et commerciaux,* LGDJ, 12e éd., 2017.

**Bitan H.**

- *Droit et expertise des contrats informatiques : Contrats de communications électroniques - Vision expertale de la protection des données*, coll. Lamy Axe droit, juin 2019.
- *Droit et expertise du numérique, Créations immatérielles, Données personnelles, E. réputation, Droit à l'oubli, Neutralité, Responsabilité civile et pénale*, coll. Lamy Axe droit, juin 2015.

**Boistel A.**

- *Cours de philosophie du droit professé à la faculté de droit de Paris* (A. Fontemoing, Paris, 1899), tome 1, *Revue internationale de l'enseignement*, 1901.

**Bourgeois M.**

- *CLOUD COMPUTING - Les défis contractuels du Cloud Computing,* JurisClasseur Communication, Fasc. 962, 1er mai 2020.

**Carbonnier J.**

- *Droit civil - Les personnes*, *Thémis*, PUF, 20e éd. 1996.
- *Droit civil - Les biens*, Tome 3, Thémis, PUF, 2000.

**Caron C.**

- *Droit d'auteur et droits voisins*, édition LexisNexis, coll. Manuels, 6e éd., septembre 2020.

**Catala P.**

- *Ebauche d'une théorie juridique de l'information, Le droit à l'épreuve du numérique,* PUF 1998.

**Castets-Renard C.**

- *Droit du marché unique numérique et intelligence artificielle*, préface de Picod F., édition Bruylant, collection droit de l'Union européenne, novembre 2020.

**Castets-Renard C., Ndior V., Rass-Masson L.,**

- *Enjeux internationaux des activités numériques, Entre logique territoriale des États et puissance des acteurs privés*, édition Larcier, collection Création Information Communication, septembre 2020.

**Colin A. et Capitant H.**

- *Cours élémentaire de droit civil français*, 11ème éd. (t.1), Dalloz 1947, mis à jour par Léon Julliot de La Morandière.

**Cornu G.**

- *Le dictionnaire vocabulaire juridique*, quadrige, Assoc. Capitant, 2020, PUF.
- *Droit civil, Les personnes*, Domat droit privé, Montchrestien, 13e éd., 2007.

**Dalloz référence Contrats du numérique**

- *Lexique anglo-français de termes de l'informatique et de l'internet*, 2021/22.

**Debet A., Massot J. et Métallinos N.**

- *Informatique et libertés : la protection des données à caractère personnel en droit français et européen*, Lextenso, 2015.

**De Terwangne C. et Rosier K.**

- *Le Règlement général sur la protection des données (RGPD/GDPR), Analyse approfondie*, Larcier, 1re édition 2018.

**Dreyer E.**

- *Droit pénal spécial,* Ellipses, 2e éd., 2012, p. 398.

**Dross W.**

- Droit civil - Les choses, LGDJ 2012.
- Droit des biens, 2e éd. LGDJ 2014.

**Eynard J.**

- *Les données personnelles, quelle définition pour un régime de protection efficace ?* Michalon, 2013.

**Fauvarque-Cosson B. et Zolynski C.**

- *Le Cloud Computing, L'informatique en nuage,* Société de législation comparée, collection Colloques, juin 2014.

**Gaudrat Ph. et Sardain F.**

- *Traité de droit civil du numérique, Tome 1 Droit des biens*, édition Larcier, 2015.
- *Traité de droit civil du numérique, Tome 2 Droit des obligations*, édition Larcier, 2015.

**Gleize B., et Maffre-Baugé A.** (sous la direction de)

- *La propriété intellectuelle renouvelée par le numérique*, édition Dalloz, Collection Thèmes et Commentaires, novembre 2020.

**Guinchard S. et Thiery Débard Th.** (sous la direction de)

- *Lexique des termes juridiques*, Dalloz, 28e éd., 2020 2021.

**Grynbaum L., Le Goffic C., Morlet-Haïdara L.**

- *Droit des activités numériques*, Dalloz, coll. Précis, 2014.

**Laroque P.**

- *Informatique et libertés publiques, in Techniques de l'Ingénieur*, Fasc. H 8770, éd. Techniques, 1970.

**Le Tourneau Ph.**

- *Contrats du numérique, informatiques et électroniques*, Dalloz référence, 12e édition, 2022-2023.

**Lucas A., Devèze J., Frayssinet J.**

- *Droit de l'informatique et de l'Internet*, *Collection Thémis Droit privé,* Presses Universitaires de France Paris, 2001.

**Netter E.** (sous la direction de)

- *Regards sur le nouveau droit des données personnelles*, CEPRISCA, coll. Colloques, novembre 2019.

**Ollard R.**

- *La protection pénale du patrimoine,* Dalloz, Nouvelle bibliothèque des thèses, tome 98, 2010.

**Perray R. et Rochfeld J.**

- *Les défis sectoriels du RGPD, Anonymisation, véhicules autonomes, eSanté, FinTechs, smart cities, AI et concurrence*, LexisNexis, septembre 2019.

**Portalis J.-E.-M.**

- *Discours préliminaire du premier projet de code civil*, 1801.

**Robin A.** (sous la direction de)

- *La propriété intellectuelle en partage*, Dalloz, Collection Thèmes et commentaires, octobre 2020.

**Roques-Bonnet M.-C.**

- *Le droit peut-il ignorer la révolution numérique* ? Michalon, 2010.

**Roubier P.**

- *Le droit de la propriété industrielle,* Tome I, édition Sirey, 1952.

**Salmon J.**

- Dictionnaire de droit international public, Bruxelles, Bruylant, 2001.

**Serge Braudo**

- Dictionnaire juridique 1996-2022 : https://www.dictionnaire-juridique.com/definition/droit-personnel.php.

**Terré F. et Simler Ph.**

- Droit des biens, Dalloz, 9e éd., 2014.

**Vivant M. et Bruguière J.-M.**

- *Droit d'auteur et droits voisins*, Dalloz, 4e éd., 2019.

**Viney G., Jourdain P. et Carval S.**,

- *Traité de droit civil, Les conditions de la responsabilité*, LGDG, 4e éd., 2013.

## II. OUVRAGES JURIDIQUES SPECIAUX : MONOGRAPHIES, COURS, THESES, MEMOIRES, RAPPORTS


**Adda H., McDermott W., Aarpi E.**

- *Le Lamy droit du numérique (Guide), Partie 6, Titre 2 Comment sécuriser les systèmes et les réseaux ?* Chapitre 1, La sécurité physique, mai 2021**.**

**Basdevant A. et Mignard JP.**

- *L'empire des données - essai sur la société, les algorithmes et la loi,* Don Quichotte éditions, mars 2018.

**Benabou L., Rochfeld J.**

- *A qui profite le clic ?* Odile Jacob, 2015.

**Benyekhlef K.**

- *La protection de la vie privée dans les échanges internationaux d'informations,* thèse, Thémis - Université de Montréal, 1992.

**Berthillon F.**

- *L'ubiquité des biens*, thèse soutenue publiquement le 18 déc. 2020, à l'Université de Lyon 3.

**Bigot Ch.**

- *Protection de la vie privée et de l'image,* Hors collection Pratique du droit de la presse, chapitre 431, 2020.

**Braibant G.**

- *Données personnelles et société de l'information, Transposition en droit français de la directive numéro 95/46*, Rapport Braibant du 3 mars 1998, La documentation française, coll. « rapports officiels », 1998, p. 7.

**Bourgeois M.**

- *Droit de la donnée, principes théoriques et approche pratique*, LexisNexis, 2017.

**Bourcier D. et Primavera De Filippi P.**

- *Open data & big data, nouveaux défis pour la vie privée*, Mare & Martin, 2016.

**Castets-Renard C.**

- *Droit de l'internet : droit français et européen*, *Montchrestien,* Lextenso éditions, 2018.

**Catala P.**

- *La propriété de l'information, Mélanges Raynaud,* Dalloz-Sirey 1985, p. 97.

**Costes L., Perray R., Adda H. (sous la direction de Costes L.)**

- *Le Lamy droit du numérique (Guide), Partie 6 - Guide, Titre 5 Comment exploiter les bases de données et les créations multimédia ? Chapitre 3 Protection de l'ensemble informationnel, Section 2 Protection des bases de données, § 3. Protection par l'action en concurrence déloyale et en parasitisme,* édition lamy expert, Wolterz Kluwer, mis à jour 04/2022.

**Coulibaly I.**

- *La protection des données à caractère personnel dans le domaine de la recherche scientifique*, thèse, Université de Grenoble, 2011.

**Debet A., Massot J., Metallinos N.**

- *Informatiques et libertés, la protection des données à caractère personnel en droit français et européen*, les intégrales, Lextenso éditions, 2015.

**Donnat F.**

- *Droit européen de l'internet : réseaux, données, services,* LGDJ, 2018.

**Féral-Schuhl Ch.**

- *Des droits de la personne renforcés*, Chapitre 112, Praxis Cyberdroit, 2020-2021.
- *Atteintes aux systèmes d'information*, chap. 712, Praxis Cyberdroit, 2020-2021.

**Gali H.**

- *Le préjudice moral en droit de la responsabilité civile*, thèse, Université Paris-Saclay, 2019.

**Ghueldre R. et Naftalski F.**

- *Le Lamy Assurances – Expert, Partie 5 E-commerce et assurance, Titre 1- Distribution de l'assurance et Internet, Chapitre 2 - Commercialisation de l'assurance par Internet,* 2 septembre 2021.

**Grosjean A.**

- *Enjeux européens et mondiaux de la protection des données personnelles,* Bruxelles, Larcier, 2015.

**Huet J. et Bouche N.**

- *Les contrats informatiques*, LexisNexis, 2011, p. 81.

**Hurpy H.**

- *Fonction de l'autonomie personnelle et protection des droits de la personne humaine dans les jurisprudences constitutionnelles et européennes*, thèse de sciences juridiques et politiques, Université d'Aix en Provence.

**Karamani-Pelacuer F., Gougot L.**

- La propriété et la possession, fiche pratique n°3209, Lexis360, 3 février 2020.

**Lajus-Thizon E.**

- *L'abus en droit pénal,* Dalloz, Coll. NBT, 2011.

**Landreau I., Peliks G., Binctin N., Pez-Pérard V., (sous la direction de Léger L.),**

- *Rapport de Génération Libre, Mes data sont à moi - Pour une patrimonialité des données personnelles,* janvier 2018 : https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf.

**Le Clainche J.**

- *L'adaptation du droit des données à caractère personnel aux communications électroniques*, thèse, Université de Montpellier I, 2008.

**Leteinturier Ch.**

- *L'information sans frontière*, 1980, la Doc. Française, Paris.

**Luciani A.-M.**

- *Les droits de la personnalité, Du droit interne au droit international*, thèse, Paris I, 1996.

**Mallet-Poujol N. (sous la direction de Vivant M.),**

- *Le Lamy droit du numérique, expert, partie 3 - Numérique et contrats, Division 3 - Les principaux contrats du numérique et leurs spécificités, Chapitre 6 - Les contrats d'informatique dématérialisée (cloud computing*), 22 avril 2022.

**McLachlan C.**

- *From Savigny to Cyberspace: Does the Internet Sound the Death-Knell for the Conflict of Laws ?* Media and Arts Law Review, 2006, vol. 11, p. 418.

**Medhioub H.**

- *Architectures et mécanismes de fédération dans les environnements Cloud Computing et Cloud Networking,* thèse, Telecom sudparis et Université Pierre et Marie curie, 2015.

**Mousseron M.**

- *Secret et contrats - de la fin de l'un à la fin de l'autre*, Mélanges Foyer, PUF,1997.

**Munari Y.**

- *L'apport du droit de l'Union européenne en droit des contrats internationaux de cloud computing*, Mémoire de master 2 droit européen des affaires, sous la direction de Mme Blandine de Clavière Professeur à l'Université Jean Moulin Lyon 3, 2016.

**Neale A.D et Stephens M.L.**

- *International Business and National Jurisdiction,* 1re éd., Oxford, Clarendon Press, 1988.

**Poullet Y.**

- *La vie privée à l'heure de la société du numérique,* 1re éd, Bruxelles, Larcier, 2019, p. 5.
- *Introduction aux aspects juridiques des contrats télématiques professionnels,* CRID, juillet 1987.

**Rochelandet F.**

- *Économie des données personnelles et de la vie privée*, collection Repères, La découverte, édition 2010.

**Saint-Gal Y.**

- *Protection et défense des marques de fabrique et concurrence déloyale*, 5e éd., Delmas, 1982.

**Testu F.X.**

- *Contrats d'affaires, chapitre 21 – Négociation et conclusion des contrats,* Dalloz référence, édition 2010.
- *Contrats d'affaires, Chapitre 121 – Traitement juridique des contrats internationaux,* Dalloz référence, édition 2010.

**Vanbrabant B.**

- *Les Contrats relatifs au savoir-faire et autres secrets d'affaire, dans Secrets d'affaires, 113, les dossiers du journal des tribunaux* (sous la direction de Vincent Cassiers), Larcier, édition 2020.

**Quéméner M., Dalle F., Wierre C.**

- *Quels droits face aux innovations numériques*, Gualino, Lextenso, 2020.

**Stirn B.**

- *Les grands avis du Conseil d'État*, Paris, LGDJ, 1997, p. 399.

**Vivant M.**

- *La contrefaçon entre contrat et délit, Réflexion sur les catégories juridique,* Mélanges en l'honneur du professeur Jacques Mestre, LGDJ, 2019, p. 931.

**Warusfel B. (sous la direction de Vivant M.),**

- Le Lamy droit du numérique, Expert, Partie 3 - Numérique et contrats, division 3 - Les principaux contrats du numérique et leurs spécificités, chapitre 6 - Les contrats d'informatique dématérialisée (cloud computing), 22 avril 2022.

**Warusfel B., Mallet-Poujol N., Costes L. (sous la direction de Vivant M.)**

- Le Lamy droit du numérique, Partie 1 Numérique et biens, Division 2 Bases de données et autres ensembles informationnels, Chapitre 2 Protection des bases de données et autres ensembles informationnels, 205 - Des données aux ensembles de données, édition lamy expert, Wolterz Kluwer, mis à jour 04/2022.

## III. OUVRAGES NON JURIDIQUES

**Acquisti A., Taylor C., et Wagman L.**

- *The Economics of Privacy,* Journal of Economic Literature, 54(2), 442–492, 2016.

**Audureau W.**

- *Ce qu'il faut savoir sur Cambridge Analytica, la société au coeur du scandale Facebook,* Le Monde, 22 mars 2018.

**Beky A.**

- Peu de services cloud conformes au futur droit européen sur les données, 13 août 2014 (en ligne) https://www.silicon.fr/fournisseurs-cloud-reglement-data-protection-europe-96121.html.

**Beck U.**

- *La société du risque. Sur la voie d'une autre modernité,* Paris, Champs Flammarion, 2003.

**Briffaut J.-P. et Stephan F.**

- *Cloud computing, évolution technologique, révolution des usages*, Lavoisier, 2013.

**Buyya R., Broberg J., et Goscinski A.M.**

- *Cloud Computing: Principles and Paradigms*, John Wiley & Sons, 2010, (en ligne) http://dhoto.lecturer.pens.ac.id/lecture_notes/internet_of_things/CLOUD%20COMPUTING%20Principles%20and%20Paradigms.pdf.

**Chee B. et Franklin C. Jr.**

- *Cloud Computing: Technologies and Strategies of the Ubiquitous Data Center*, CRC Press, 2010.

**Fagot V.**

- *Et si chacun vendait ses données personnelles sur Internet ?* Le Monde, 26 janvier 2018.

**Hidalgo C.**

- *Why information grows: The evolution of order, from atoms to economies,* Basic Books, 2015.

**Locke J.**

- *Second Treatise of Government,* Chapter 5: Property, 1690.

**Mahmood Z. et Hill R.**

- *Cloud Computing for Enterprise Architectures*, Springer, 2011.

**Proudhon P-J**.

- *Théorie de la propriété* (1862), L'Harmattan Éditeur, 1997.

**Rigaux F. et Delpérée F.**

- *Le concept du peuple,* 1re éd., Bruxelles, Story-Scienta, 1988, p. 216.

**Winkler V.J.R.**

- *La sécurité dans le Cloud. Techniques pour une informatique en nuage sécurisée*, Pearson, Paris, 12 octobre, 2011.

**IV. CHRONIQUES ET ETUDES**

**Andry F.**

- *Cloud et plateformes : pourquoi ces technologies ont-elles autant d'impact ?* Dalloz IP/IT, publié le 1er juin 2020, n° 6, p. 344-351.

**Ancel M.-E.**

- *D'une diversité à l'autre, À propos de la « marge de manœuvre » laissée par le Règlement général sur la protection des données aux États membres de l'Union européenne,* Rev. crit. DIP 2019. 647.

**Antin O. et Brossollet L.**

- *Le domaine de la vie privée et sa délimitation jurisprudentielle*, Légicom, octobre 1999, n° 20, pp. 9-19.

**Augagneur L-M.**

- *Héberger ses données chez les GAFAM : quel discours croire sur le Cloud Act ?* Revue Lamy Droit de l'Immatériel (nº 162), 1er août 2019.

**Auroy B.**

- *Le vol de données informatiques ou l'avènement de la « soustraction 2.0 »,* Revue Lamy Droit de l'Immatériel, Nº 120, 16 novembre 2015.

**Badinter R.**

- *Le droit au respect de la vie privée*, JCP G, 1968, I, 2136, n° 12.

**Banck A.**

- GDPR et sous-traitance : un nouveau devoir de conseil ? Dalloz IP/IT, 2017.

**Beignier B.**

- *Vie privée et vie publique*, Légipresse, sept. 1995, n° 124, pp. 67-74.

**Benabou V.-L.**

- L'extension du domaine de la donnée, Légipresse, 1er avril 2018, n° 359, p. 197-207.

**Benyahia N.**

- *Établissements de santé et start-up face à la régulation des innovations par la protection des données de santé,* journal de Droit de la Santé et de l'Assurance Maladie (JDSAM), 1er juillet 2018, n° 20, p. 21-2.

**Behar-Touchais M.**

- *La réforme du titre IV du livre IV du code de commerce,* JCP E 2019. 1361.
- *L'effectivité du droit face à la puissance des géants de l'Internet,* IRJS-éditions, 2015, p. 73.

**Benabou V-L.**

- *Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ?* RTD Eur. 2021 p.279.
- *Le RGPD ou la ligne Maginot de la protection des données personnelles face aux acteurs extra-européens ?* Rev. Mar. Un. Européen, 2021.

**Bérard M.-H., Lamy P., Vimont P., Schweitzer L. et Fatah F.**

- *L'Europe face aux sanctions américaines, quelle souveraineté ?* Policy Paper n° 232, Institut Jacques Delors, 23 octobre 2018.

**Bergé J.-S. et Grumbach S.**

- *La sphère des données et le droit : nouvel espace, nouveaux rapports aux territoires*, JDI, 2016, pp. 1153-1173.

**Bernault C.**

- *Informatique en nuage et données personnelles : quand l'informatique est dans les nuages, les données personnelles s'envolent !* RLDI 2012/78, nº 2616.

**Bernelin M.**

- *Etude 1172, La patrimonialisation des données personnelles : entre représentation(s) et réalité(s) juridiques,* JCP G 2019.

**Berthet C., Zolynski C.**

- *L'empouvoirement des citoyens de la République numérique regards sur une réforme en construction,* RLDI 2018/1, n° 144, p. 60, spéc. n° 14.

**Bertrand B.**

- *La volonté de réguler les activités numériques*, Chronique Droit européen du numérique, RTD Eur. 2021 p.160.
- *La confiance numérique,* Chronique Droit européen du numérique, RTD Eur. 2021 p.153.
- *Polyphonie dans l'appréciation du recours à une solution technique américaine pour la Plateforme Health Data Hub : le Conseil d'État et l'art de la fugue,* JCP n° 49, 30 nov. 2020, 1358.

**Bertrand R. A.**

- *Droits de l'auteur*, chapitre 106, Dalloz action Droit d'auteur, 2010.

**Binctin N.**

- *Savoir-faire*, *Répertoire IP/IT et Communication*, Janvier 2018.
- *Marque - Droit pénal de la contrefaçon, Répertoire de droit commercial,* Dalloz, Octobre 2020 (actualisation : Mai 2022).

**Bloch C.**

- *La cessation de l'illicite, Recherche sur une fonction méconnue de la responsabilité civile extracontractuelle*, Dalloz, 2008.

**Boev I.**

- *Le nouveau règlement : un 5e principe de libre circulation ?* Dalloz IP/IT 2020.

**Borra P.**

- *La notion de dépendance économique en droit français*, AFEC, Journée du 8 janvier 1993, p. 31.

**Bougeard A.**

- *Les dispositions relatives à l'accès et au portage des données : code de conduite et bonnes pratiques,* Dalloz IP/IT 2020 p. 408.

**Bounedjoum A.**

- *Réforme européenne des données personnelles : les nouveautés pour les droits des personnes :* JCP E 2016, 1327.

**Bourdoiseau J.**

- *DataJust ou la réforme du droit de la responsabilité civile à la découpe ?* Lexbase Hebdo, Edition Privée Générale, 23 avril 2020, numéro 821.

**Brault D.**

- *Politique et pratique du droit de la concurrence en France*, LGDJ Droit des affaires, 2004, n° 946.

**Brunaux G.**

- *Cloud computing, protection des données : et si la solution résidait dans le droit des contrats spéciaux ?* D. 2013, Chron. p. 1158.

**Buy F.**

- *La [décevante] réforme du droit des relations commerciales*, D. 2019. 1122.

**Campagne N.**

- *La protection informatique et libertés des données des personnes morales en Europe*, RLDI, nº 104, 1er mai 2014.
- *Du bon usage des règles informatique et libertés pour les fichiers d'entreprises*, RLDI nº 107, 1er août 2014.
- *Réalité et limites de la protection de la vie privée des entreprises*, RLDI, nº 101, 1er février 2014.

**Caprioli E**.

- *Contrats de prestations informatique : quelques précautions juridiques*, Mag Securs n°45, p.19-20, 2015.

**Carre S.**

- *Libre circulation des données, propriété et droit à l'information : à propos du règlement (UE) 2018/1807 du 14 novembre 2018,* Dalloz IP/IT 2020.

**Castets-Renard C.**

- *Schrems II et invalidation du Privacy Shield, un goût de « déjà vu »*, Recueil Dalloz, D. 2020. 2432.

**Castex L.,**

- *Les éternités numériques un essai d'analyse prospective,* RLDI 2016/11, p. 49, spéc. II.

**Cervetti D.**

- *La personne morale (encore) évincée de la qualité d'auteur,* RLDI n° 114, 1er avril 2015.

**Chadelat C., Valdès-Boulouque M.**

- *Mission d'évaluation du dispositif législatif et réglementaire des ventes volontaires de meubles aux enchères publiques*, ministère de la justice déc. 2014, p. 30.

**Chagny M.**

- *Quelle refonte du Titre IV du Livre IV du code de commerce après l'ordonnance no 2019-359 du 24 avril 2019 ?* JCP E 2019. 304.

**Chamoux J.-P.**

- *Impacts économiques et juridiques de l'informatisation,* Paradoxes 1982, p. 116.

**Chantepie G.**

- *L'inexécution du contrat de cloud computing*, RLDI 2013/98, p.117.

**Chantepie G., Sauphanor-Brouillaud N.**

- *Déséquilibre significatif, Répertoire de droit civil,* Dalloz janvier 2022 (actualisation : Mars 2022).

**Chassigneux C.**

- *Aterritorialité des atteintes face aux logiques territoriales de protection juridique et problème de l'absence d'homogénéité des législations protectrices (quid des safe harbor principles),* Lex Electronica, vol. 9, n° 2, Numéro Spécial, 2004.

**Chatry S.**

- *La légitimité du droit sui generis du producteur de bases de données,* Légipresse 2019.

**Chavernoz A. et Goupil C.**

- *Contrats cloud : quels points d'attention dans la négociation ?* La Semaine Juridique Edition Générale n° 23, 7 juin 2021, 627.

**Cluzel-Métayer L.**

- *La loi pour une République numérique : l'écosystème de la donnée saisi par le droit,* AJDA 2017.

**Cordier G.**

- *Le contrat ASP*, Comm. Com. électr. 2008, n° 10, prat.9.
- *Focus sur la directive n° 2009/136/CE du 25 novembre 2009*, RLDI 2010/57, n° 1904.

**Cordier G., Kennedy J. et Ritchie M.**

- *Les contrats d'outsourcing en temps de crise : une approche internationale :* comm. com. électr., févr. 2009, fiche pratique, p. 50.

**Crichton C.**

- *Création de DataJust, un algorithme prédictif d'évaluation du préjudice*, Dalloz IP/IT, 1er avril 2020, n° 4, 209-209.

**Curto J.**

- *La fin justifie-t-elle les moyens ? De la notion de vie privée et de la preuve déloyale*, Revue Lamy Droit Civil, avr. 2012, n° 92, pp. 55-56.

**Danis-Fatôme A.**

- *Etude, Protection des données - Quelles actions judiciaires en cas de violation du RGPD ?* Communication Commerce électronique n° 4, Avril 2018, dossier 18.

**Dèbes V. F.**

- *Une page se tourne pour le cloud souverain français,* Les Échos, 1er août 2019.

**Debet A.**

- *L'invalidation du Safe Harbor par la CJUE : tempête sur les transferts de données vers les États-Unis*, La Semaine Juridique Edition Générale, n° 46-47, 9 novembre 2015, 1258.

**Decocq A. et Pédamon M.**

- *L'ordonnance du 1er décembre 1986 relative à la liberté des prix et de la concurrence*, J.-Cl. Conc. consom., no spéc. 1987, no 28.

**Delaunay B.**

- *L'open data dans les collectivités territoriales,* La Semaine Juridique Administrations et Collectivités territoriales n° 42, 22 octobre 2018, 2286.

**Delmas-Linel B. et Mutz C.**

- *Les sept recommandations de la CNIL en matière de cloud computing : nécessaires, mais pas suffisantes*, RLDI 2012/85, nº 2871.
- *Le cloud computing à l'épreuve des souverainetés nationales. Faut-il avoir peur du USA Patriot Act ?* RLDI, février 2013, p.53.

**Delmas-Marty M.**

- *Le relatif et l'universel. Les forces imaginantes du droit*, Ed. du Seuil, 2004, p. 337.

**De Mello X.**

- *Dépendance économique ou position dominante ?* AFEC, Journée du 8 janvier 1993, p. 37.

**Deroudille A. et Fatah. F.**

- *L'extraterritorialité du RGPD dans le contexte du « Cloud Act »,* Rev. UE 2019. n°442.

**Deschanel C.**

- *L'instauration d'un droit de propriété des données personnelles ? vrai danger ou fausse utilité ? RLDI n° 156, 2019, n° 5344.*

**Desrumaux N., Sénéchal J., Poidevin B., Cruquenaire A., Cassart A., Chantepie G., Dubois. N., Hellendorff C., Roques-Bonnet M.-C., Naftalski F.**

- Contrats et cloud computing, RLDI 2013/98, nos 3267 à 3275.

**Destreguil M.**

- *Plaidoyer en faveur d'une approche propriétariste des données personnelles*, *RJFP* n° 3, 2019.

**Detraz S.**

- *Vol de données informatiques*, Gaz. Pal. 2015, no 169, p. 8.

**Deumier P., Sorel J.-M.**

- *Regards croisés sur la soft law en droit interne, européen et international,* LGDJ, 2018, p. 55-76, v. p. 63.

**De Roumeforts S.**

- *Déséquilibre significatif : premières précisions de la Cour de cassation depuis la réforme de 2016,* Revue Lamy Droit civil, Nº 201, 1er mars 2022.

**De Roux H., Zilberman A.**

- *La loi sur le secret des affaires : un premier élan vers la protection des données sensibles des entreprises françaises ?* Revue Lamy droit des affaires, Nº 141, 1er octobre 2018.

**Destreguil M.**

- *Plaidoyer en faveur d'une approche propriétariste des données personnelles,* RJPF 2019, nº 3.

**Dormont S.**

- *Droits patrimoniaux,* Répertoire IP/IT et Communication, droit d'auteur, septembre 2019.

**Dreyer E.**

- *Consécration provisoire du vol de données informatiques,* AJ pénal, 2015. 413.

**Dumoulin L.**

- *Les droits de la personnalité des personnes morales*, Revue des sociétés Dalloz, 2006.

**Eggrickx B. et Jouffin E.**

- *Cloud Act : nouvelle manifestation de l'extraterritorialité des textes US et réponse européenne,* Banque et Droit, hors-série, mars 2019.

**Eréséo N.**

- *Libre circulation des données et droit de la concurrence* (à propos du règlement du 14 novembre 2018 relatif à la libre circulation des données non personnelles), Dalloz IP/IT, 2020 p.414.

**Ettighoffer D.C.**

- *L'économique numérique sera-t-elle sous domination américaine ?* Géoéconomie 2010/2 (n° 53), pages 89 à 99.

**Eynard J. et M. Monteil M.**

- *Le CEPD apporte des précisions sur la notion de transfert international de données,* Dalloz actualité, 1er décembre 2021.
- *Transferts de données : le CEPD revient sur les conséquences de l'arrêt Schrems II* –Dalloz actualité, 7 juillet 2021.
- *Limitations aux droits des personnes concernées : les lignes directrices du CEPD,* Dalloz actualité, 10 novembre 2021.

**Faculté de droit et des sciences sociales de Poitiers**

- *Actes & Colloques, Le principe de l'article 2 § 1 de la Charte des Nations Unies, Entre théorie et pratique*, 14 janvier 2014.

**Favro K.**

- *Les données non personnelles : un nouvel objet juridique,* Dalloz IP/IT 2020.

**Favro K., Zolynski C.**

- *DSA, DMA : L'Europe encore au milieu du gué,* Dalloz IP/IT 2021. 217.

**Fouilland F.**

- *L'auteur personne morale, éléments pour une théorie de l'emprunt de personnalité artistique,* Comm. com. électr. 2008, nº 12, étude 24.

**Flipo O. et Forest D.**

- *Contrats : la disponibilité dans les contrats SaaS*, Expertises 2012.

**Galloux J.-C.**

- *Ebauche d'une définition juridique de l'information*, 1994, Dalloz chron., p. 229-234.

**Gavalda C.**

- *Le secret des affaires*, Mélanges René Savatier, Dalloz, 1965, p. 291.

**Gauvain R.**

- *Rapport parlementaire sur les procédures extraterritoriales,* Revue Lamy droit des affaires, Nº 157, 1er mars 2020.

**Ginossar S.**

- *Pour une meilleure définition du droit réel et du droit personnel,* RTD civ. 1960, p37.

**Griguer M.**

- *Droit d'accès, droit à la portabilité : quelles différences ?* Comm. com. électr. 2018, dossier 14.

**Grossa J.**

- *Les données non personnelles : un tech checking,* Dalloz IP/IT 2020.

**Guerrier C.**

- *La LOPPSI 2 en 2011*, RLDI 2011/70, nº 2325.

**Guichardaz R. et Pénin J.**

- *L'économie de la réutilisation des données (non personnelles),* Dalloz IP/IT 2020.

**Hagel F.**

- *Secret et droits de propriété intellectuelle : un tour d'horizon*, RLDI 10/2009, n° 53.

**Hoeren T.**

- *Big Data and the Ownership in Data: Recent Developments in Europe,* European Intellectual Property Review 2014, p. 751.

**Huet J.**

- *Contrats informatiques - Contenu et typologie, Fascicule 322,* JurisClasseur Commercial, 20 mars 2013.

**Jacob P.**

- *La compétence des États à l'égard des données numériques : du nuage au brouillard... en attendant l'éclaircie ?* Rev. crit. DIP 2019. 665.

**Johnson D.R et Post D.**

- *Law and Borders – The Rise of Law in Cyberspace,* Stan. L. Rev., 1995, vol. 48, p. 1367.

**Jouffin E.**

- *Recommandations de l'ABE en matière de cloud computing-Un texte mort-né ?* Revue Banque et Droit, 1er septembre 2018, numéro 181, page(s) 32-35.

**Jouffin E., Lemarteleur X. et Gibon M.-N.**

- *Le Règlement sur la Protection des données : les 10 Commandements à connaître pour passer de la théorie à la pratique :* RD bancaire et fin. 2016, étude 18.

**Kayser P.**

- *Les droits de la personnalité. Aspects théoriques et pratiques*, RTD civ. 1971. 445, spéc. n° 35.
- *La protection de la vie privée par le droit, protection du secret de la vie privée*, *Économisa*, Presses Universitaires d'Aix-Marseille, 2e édition, 1990.

**Kornbeck J.**

- *Droit dur ou mou ? L'Union européenne et la promotion des APS,* Jurisport 2021, n°216, p.39.

**Lacroix-De Sousa S.**

- *Les sociétés face au RGPD : les enjeux de la compliance,* Revue des sociétés 2021, no 6, p. 351.

**Lanier J., Arrieta Ibarra I., Goff L., Jimenez Hernandez D., Weyl E. G.**

- *Should We Treat Data as Labor? Moving Beyond « Free »* (traduction : " Devrions-nous traiter les données comme de la main-d'œuvre ? Au-delà de la "gratuité") Vol.1 N°1, Mai 2018 (en ligne) https://ssrn.com/abstract=3093683).

**Laulom S.**

- *L'indépendance affirmée de l'article 9 du Code civil du droit commun de la responsabilité,* D. 1997, p. 403.

**Lavenue J.-J.**

- *Internationalisation ou américanisation du droit public : l'exemple paradoxal du droit du cyberspace confronté à la notion d'ordre public*, Lex Electronica, Volume 11, Numéro 2,2006.

**Lapotre C.**

- *Actualité jurisprudentielle en matière de données personnelles : La Cour de justice se pose en gardienne des droits fondamentaux des citoyens de l'Union européenne*, la Revue du journal du management juridique et réglementaire, n° 79 novembre-décembre 2020.

**Lassalle M.**

- Étude, *Droit à l'autodétermination informationnelle — La réparation des atteintes au droit à l'autodétermination informationnelle*, Communication Commerce électronique n° 2, février 2021, étude 4.

**Le Cam S.**

- Droit d'auteur et les droits voisins dans le marché unique numérique : projet de loi ratifiant l'ordonnance du 24 novembre 2021, Dalloz actualité, 14 mars 2022.

**Leclercq P.**

- *Essai sur le statut juridique des informations,* ministère de la Justice, 1980.

**Lepage A.**

- *Faux profil sur Facebook,* Comm. Com. Élec., 2011, comm. 28.
- *Droits de la personnalité* juillet 2006 – juillet 2007, Recueil Dalloz 2007, p. 2771.

**Le Quellenec E.**

- *L'émergence d'un cloud souverain européen*, RLDI, 1er août 2020, numéro 173, page(s) 37-39.

**Le Quellenec E., Huin L., Benchetrit A., Korabelnikov D.**

- *Cloud computing et droit, retour sur une année de grands changements,* RLDI, Nº 138, 1er juin 2017.

**Loiseau G.**

- *Des droits patrimoniaux de la personnalité en droit français*, McGill Law Journal 1997, p. 319.

**Maisnier-Boché L.**

- *Droit à l'effacement, à la rectification, à la limitation et droit d'opposition dans le Règlement européen,* Comm. com. électr. 2018, comm. 14.

**Malaurie Ph.**

- *Les précédents et le droit,* Revue internationale de droit comparé, 2006, 58-2 pp. 319-326.

**Mallet-Poujol N.**

- *Appropriation de l'information : l'éternelle chimère :* D. 1997, Chron. p. 330.

**Mantovani M.**

- *Le RGPD en tant qu'espace juridique multi-échelle : quelles implications pour le droit international privé ?* Revue de droit international d'Assas n° 2, déc. 2019, p. 4.

**MarcellinY.**

- La protection pénale de la contrefaçon de marques et de dessins et modèles, RDPI 1996 no 63 p. 24.

**Martin L.**

- *Le secret de la vie privée*, RTD civ. 1959. 227, spéc. p. 230.

**Martial-Braz N.,**

- *Les nouveaux droits des individus consacrés par la loi pour une République numérique, Quelles innovations ? Quelle articulation avec le règlement européen ?* Dalloz IP/IT, nov. 2016, p. 525 et s.

**Martin L.**

- *Le secret de la vie privée*, RTD civ. 1959, 227.

**Matsopoulou H. et Mascala C.**

- *L'action pénale en contrefaçon en général,* Le Lamy droit pénal des affaires, Mis à jour 11/2021.

**Mattatia F.**

- *Synthèse du futur règlement européen sur les données personnelles (1re partie) : principaux généraux et obligations du responsable de traitement :* RLDI 2016/126, no 3985.

**Mattatia F. et Yaïche M.**

- *Etre propriétaire de ses données personnelles : peut-on recourir au régime traditionnel de propriété ?* RLDI, 2015/114.

**Mendoza-Caminade A.**

- *La présomption de préjudice en matière de concurrence déloyale et de parasitisme,* La Semaine Juridique Edition Générale n° 22, 31 mai 2021.
- *Internet et compétence juridictionnelle : (enfin) la fin de la compétence universelle du juge français*, LPA 8 nov. 2007, n° PA 200722402.

**Metallinos N**.

- *Les critères de la qualification des acteurs :* Comm. com. électr. 2018, dossier 8.
- Introduction d'une action de groupe en matière de violation de la loi Informatique et Libertés: Comm. com. électr. 2016, comm. 95, spéc. p. 40.

**Mestre J.**

- *La protection, indépendante du droit de réponse, des personnes physiques et des personnes morales contre l'altération de leur personnalité aux yeux du public,* JCP 1974. I. 2623.

**Métille S.**

- *L'utilisation de l'informatique en nuage par l'administration publique,* AJP/PJA, juin 2019.

**Mihman A., Lucas De Leyssac M.-P.**

- *Vol simple : ses composantes*, Répertoire de droit pénal et de procédure pénale, Avril 2016.

**Motahareh F. B., Rivollier V.**

- *À propos de DataJust : justesse de l'outil numérique, juste indemnisation des victimes ?* RLDC, 1er septembre 2020, numéro 184, page(s) 18-24.

**Mouchette J.**

- *Haro sur les obligations de localisation des données non personnelles*, Revue Dalloz IP/IT 1er juillet 2020, numéro 7, page(s) 401-407.

**Mousseron J.-M. et Sélinsky V.**

- *Le droit français nouveau de la concurrence*, Litec, 1987, no 123.
- *Montagne ou souris : commentaire de la loi du 30 décembre 1985 portant amélioration de la concurrence*, JCP E 1986, II, no 14682.

**Muller É.**

- La libre circulation des données et la directive concernant la réutilisation des données du secteur public, Dalloz IP/IT 2020 p.424.

**Naftalski F.**

- *Les BCR « sous-traitants » consacrés par le Groupe de l'article 29 : un grand pas en avant pour sécuriser les transferts internationaux de données dans le cadre du cloud computing*, RLDI 2012/85, nº 2870.

**Naftalski F. et Desgens-Pasanau G.**

- *Le cloud computing à l'épreuve des souverainetés nationales*, RLDI 2013/90, nº 3006.

**Netter E., Ndior V., Puyraimond J-F, Vergnolle S.**

- *Regards sur le nouveau droit des données personnelles,* Centre de droit privé et de sciences criminelles d'Amiens, 2019, 979-10-97323-05-9. hal-02357967.

**Ochoa N.**

- *Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition,* RFDA 2015. 1157.

**Padova Y.**

- *Entre patrimonialité et injonction au partage : la donnée écartelée ?* (Partie I), Revue Lamy Droit de l'Immatériel, Nº 155, 1er janvier 2019.

**Pailler L.**

- *Pas de droit fondamental à la protection des données pour les personnes morales,* Revue Lamy Droit de l'Immatériel, nº 177, 1er janvier 2021.
- *L'applicabilité spatiale du Règlement général sur la protection des données (RGPD) :* Commentaire de l'article 3, JDI, 2018.

**Pasqui G.**

- *L'abus de dépendance économique*, Rev. conc. consom. 1993, no 71.

**Pedamon M.**

- *Les abus de domination*, Cah. dr. entr. 1987/1, p. 15.

**Peltier V.**

- *Le secret des correspondances,* PUAM, 1999, nº 757, p. 595.

**Petel A.**

- *Publication de l'Acte sur la gouvernance des données : les propositions de la Commission européenne, quels sont les points clés de la proposition d'Acte sur la gouvernance des données ?* Revue Lamy Droit de l'Immatériel, Nº 176, 1er décembre 2020.
- *L'« Acte sur la gouvernance des données » : l'Union européenne dévoile le premier pilier du marché européen des données,* La Semaine Juridique Edition Générale n° 22, 6 Juin 2022, 698.

**Pirovano A. et Salah M.**

- *L'abus de dépendance économique : une notion subversive* ? LPA 24 sept. 1990.

**Poggi A.-S. et Lefèvre A.**

- *Les offres Cloud pour entreprises et la protection des données à caractère personnel : les recommandations dont les entreprises doivent tenir compte lorsqu'elles choisissent une offre Cloud,* RLDI 2014/106, no 3532, pp. 44-50.

**Poidevin B.**

- *Le contenu du contrat de cloud computing*, RLDI, 1er novembre 2013, numéro 98, page(s) 104-107.

**Poullet Y.**

- Introduction aux aspects juridiques des contrats télématiques professionnels, CRID, 1989.

**Poster A.R.**

- *An economic Theory of Privacy*, Regulation, vol.2, n° 19, 1978.

**Purtova N.**

- *Property Rights in Personal Data. A European Perspective,* Kluwer Law International 2012.

**Quéméner M.**

- *La loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2) au regard des nouvelles technologies*, Comm. Com. Électr., 2011, chron. 9.

**Quiquerez A.**

- *Actualité du droit des technologies nouvelles (février-juin 2020)*, Revue Lamy Droit Civil, 1er septembre 2020, numéro 184, page(s) 25-36.

**Quiviger P.-Y.**

- *Une approche philosophique du concept émergent de souveraineté numérique,* NCCC 2017, n° 57, p. 25.

**Ragheno N.**

- *Data Protection & Privacy. Le GDPR dans la pratique/De GDPR in de praktijk,* RLDC, 14 juin 2018, numéro 2, page(s) 307-310.

**Rambaud S.**

- *Droit sui generis des bases de données : vers un équilibre ?* Revue Lamy Droit de l'Immatériel, N° 49, 1er mai 2009.

**Robin A.**

- *Le principe d'ouverture des données de la recherche scientifique*, Revue Intelligibilité du numérique, 1|2020. [En ligne] https://doi.org/10.34745/numerev_1690.
- *L'ouverture des données publiques scientifiques : de l'examen de la règle « open as possible, closed as necessary »,* Communication Commerce électronique n° 9, Septembre 2020, étude 15.

**Robin C.**

- *L'exploitation abusive d'un état de dépendance économique*, LPA 28 juill. 2 août 1989.

**Rozenfeld S.**

- *Le Cloud Act : pour un accès extraterritorial aux données*, Revue Expertises des systèmes d'information, 1er avril 2018, numéro 434, page(s) 123-124.

**Saint-Aubin Th.**

- *Les nouveaux enjeux juridiques des données (big data, web sémantique et linked data), Les droits de l'opérateur de données sur son patrimoine numérique informationnel,* RLDI, n° 102, 1er mars 2014.

**Saint-Gal Y.**

- *Concurrence déloyale et concurrence parasitaire*, RIPIA, 1956. p.19.

**Saenko L.**

- *Vol par téléchargement de données numériques*, D. 2015. 1466.

**Sauron J.-L.**

- *Le règlement général sur la protection des données, règlement (UE) n° 2016/679 du 27 avril 2016 : de quoi est-il le signe* ? Comm. com. électr. 2016, étude 16.

**Schütz R.-N.**

- *Inaliénabilité*, Répertoire de droit civil, Juin 2014 (actualisation : Octobre 2020).

**Schmid Ch., Nadakavukaren Schefer K. et Heckendorn Urscheler L.**

- *Conflict of laws in the maze of digital platforms - Le droit international privé dans le labyrinthe des plateformes digitales*, actes de la 30e Journée de droit international privé du 28 juin 2018 à Lausanne, n°86, L'Institut suisse de droit comparé, Edition Romandes Schulthess, 2018.

**Sélinsky V.**

- *Abus de domination*, J.-Cl. Cons. conc., Fasc. 315, 1992, no 82.

**Sordet E. et Milchoir R.**

- *Le cloud computing, un objet juridique non identifié ?* Communication commerce électronique 2011, étude n° 20.
- *La définition des contours juridiques du cloud computing*, Communication commerce électronique, novembre 2012.

**Targa A.**

- *La notion d'atteinte à la concurrence sur le marché en droit français*, Rev. conc. consom. 1993, comm. 76.

**Thierache C.**

- *RGPS vs Cloud Act : le nouveau cadre légal américain est-il anti RGPD ?* Dalloz IP/IT, juin 2019, n° 6, p. 367.

**Thréard J. et Bourgeon Ch.**

- *Dépendance économique et droit de la concurrence, réflexions sur l'article 8 de l'ordonnance du 1er décembre 1986*, Cah. dr. entr. 1987, Fasc. 2, p. 20.

**Traullé J.**

- *L'éviction de l'article 1382 du Code civil en matière extracontractuelle*, LGDJ, 2007.

**Türk P.**

- *La souveraineté des États à l'épreuve d'internet,* RD publ. 2013. 1489.

**Uzan-Naulin J. et Perray R.**

- *La nouvelle norme simplifiée de la CNIL en matière de clients, prospects et vente en ligne : entre convergence, cohérence et conformité,* Comm. com. électr. 2017, étude 2.

**Vivant M.**

- *La contrefaçon entre contrat et délit, Réflexion sur les catégories juridique*, Mélanges en l'honneur de Jacques Mestre, LGDJ, Juillet 2019, p. 931
- *La privatisation de l'information par la propriété intellectuelle*, Revue internationale de droit économique 2006/4 (t. XX, 4), pages 361 à 388.

**Wagener N.**

- *Cloud souverain* et archives publiques, JAC 2017, n° 43, p. 38.

**Warren S. et Brandeis L.**

- *The right to privacy,* Harvard Law Review, 1890, vol. 4, nº 5, p. 193-220.

**Watin-Augouard M.**

- *La cybersécurité, enjeu de la souveraineté à l'ère numérique,* Dalloz IP/IT 2021, p.130.

**Westin A.**

- *Privacy and freedom*, *Atheneum*, 1967.

**Witz G. et Mariez J.-S.**

- Les données publiques au cœur de l'IA et au service de la ville intelligente, Revue Lamy droit des affaires, Nº 151, 1er septembre 2019.

**Zolynski C.**

- *Quelle circulation des données non personnelles pour l'Union européenne ?* Revue des affaires européennes, 1er janvier 2018, numéro 1, page(s) 73-78.
- *La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne,* Dalloz IP/IT 2020 p.429.

## V. CONTRIBUTIONS A DES COLLOQUES

**Ceyhan A., Garapon A. et Michaël Foessel M.**

- *Séminaire IHEJ/Esprit* du 20 mars 2006.

**Martial-Braz N. et Martine Behar-Touchais** (sous la direction de)

- *L'effectivité du droit face à la puissance des géants de l'internet*, *Le droit des contrats à l'épreuve des géants d'internet*, page 69, Tome 63, vol. 1 actes des journées du 14,15 et 16 octobre 2014, Collection Bibliothèque de l'IRJS -André Tunc.

**Mendoza-Caminade A.**

- *Le rôle du sous-traitant en matière de données personnelles. In : Actes de colloques de l'IFR, Sécuriser la sous-traitance : quels nouveaux défis ?* Presses de l'Université Toulouse 1 Capitole.

## VI. JURISPRUDENCES ET NOTES

*(classées par ordre chronologique)*

### A. Décisions de la Cour de cassation

- **Cass. com., 17 mars 2021,** pourvoi n° 19-10.414, inédit, JurisData n° 2021-003856.
- **Cass. com., 4 décembre 2019**, pourvoi n° 17-20.032, inédit**.**
- **Civ. 1re, 16 mai 2018**, pourvoi n° 17-11.210, inédit.
- **Cass. com., 20 décembre 2017**, pourvoi n° 16-18.280, inédit.
- **Cass. com., 25 janvier 2017**, pourvoi n° 15-23.547, D. 2017. 481, note Buy F.
- **Cass. 1re civ., 3 novembre 2016**, pourvoi n° 15-22.595, JurisData n° 2016-022669, JCP G 2016, 1310, R. Perray.
- **Cass. 1re civ., 17 mars 2016**, pourvoi n° 15-14.072, P I, n° 67 ; D. 2016. 1116, note G. Loiseau.
- **Cass. com., 9 février 2016**, pourvoi n° 14-23.006, JurisData n° 2016-002016.
- **Cass. com., 29 septembre 2015**, pourvoi n° 13-25.043, inédit.
- **Cass. crim., 20 mai 2015**, pourvoi n° 14-81.336, inédit.
- **Cass. com., 3 mars 2015**, pourvoi n° 14-10.907, inédit.
- **Cass. com., 3 mars 2015**, pourvoi n° 15-27.525, AJCA 2015. 218, note Chantepie**.**
- **Cass. 1re civ.,** 15 janv. 2015, pourvoi n° 13-23.566, bull.2015, I, n° 11.
- **Cass. com., 25 juin 2013,** pourvoi n°12-17.037, P: D. 2013. 1867, note Beaussonie; RTD civ. 2013. 595, obs. Barbier ; JCP 2013, no 930, note Debet; RDC 2013. 119, note Rochfeld.
- **Cass. 1re civ., 22 septembre 2011**, pourvoi n°10-23.073, inédit.
- **Cass. crim., 20 octobre 2010,** pourvoi n° 09-88.387, inédit, Caprioli E., Comm. Com. Élec., 2011, comm. 30.
- **Cass. com., 23 mars 2010,** pourvoi n° 08-20.427, 08-21.768, inédit.
- **Cass. crim., 4 mars 2008**, pourvoi n° 07-84.002, inédit.
- **Cass. crim., 9 septembre 2003**, pourvoi n° 02-87.098, inédit.
- **Cass. 1re civ., 3 juillet 1996,** pourvoi n°92-18.627, JCP E 1997, I, n° 657, no 5, obs. Vivant M. et Le Stanc Ch., D. 1997, jur., p. 328, note Françon.
- **Cass. 1re civ., 11 juin 1996**, pourvoi n°94-18.250. Bull. civ. I, n° 245.
- **Cass. crim., 23 mai 1995**, pourvoi n°94-81.141, Bull. crim., nº 193, p. 524.
- **Cass. 1re civ., 24 mars 1993**, pourvoi n°91-16.543, 2e espèce, JCP G 1993, II, n°22085, note Greffe P., RIDA 1993, n°158, p. 200.
- **Cass, Ass. Plén. du 12 juillet 1991**, pourvoi n°90-13.602, Bull. Ass. plén. n° 5, Besse c/ Protois BIF.
- **Cass. crim., 5 septembre 1989**, pourvoi n° 88-83470, CNC c/ Consorts Sudre, RTD Com. 1990 p.388 ; Rida n° 144 avr. 1990, p. 201.
- **Cass. 1re civ., 8 nov. 1988**, pourvoi n° 86-13.264, JCP 1989. II. 21301, note R. Brichet, RTD com. 1989. 92.
- **Cass. crim., 12 décembre 1984**, pourvoi n° 82-91.989, Bull.crim n° 403.
- **Cass. crim., 12 octobre 1976**, pourvoi n°75-90.239, Bull. crim. n°287.
- **Cass. crim., 12 juin 1974**, pourvoi n° 73-90.724, Ann. propr. ind. 1974. 97, PIBD 1974, III, p.399.
- **Cass. crim., 20 juin 1973**, pourvoi n° 72-92.270, Ann. propr. ind. 1974. 85.
- **Cass. 3e civ., 18 avril 1972,** pourvoi n°71-10.660, Bull.civ.III, n° 237.
- **Cass. 1re civ., 2 novembre 1966**, pourvoi n°64-12.907, Bull. civ. I, no 489.
- **Cass. 3e civ., 13 juillet 1966**, pourvoi n° 64-12,946, Bull.civ.III, n° 358, p.316, JCP éd G 1967, II, n° 15131, note Durand P.
- **Cass. crim., 29 juin 1960**, Bull. crim. p. 350.
- **Cass. crim., 14 mai 1958**, Bull. crim. nº 391 ; D.1958. 513 (1re esp.), note M.R.M.P ; Gaz. Pal. 1958. 2. 18; S. 1958. 303.

- **Cass. crim., 29 mars 1935**, Bull. crim., p.350.
- **Cass. crim., 4 juin 1915**, Bull. crim. nº 121.
- **Cass. 1re civ., 4 mai 2012**, pourvoi n° 10-27.208, Gaz. Pal., 17 mai 2012, no 138, p. 13.
- **Cass. crim., 16 mai 1862**, Ann. propr. ind. 1862 p.221.

**B. Décisions du Conseil constitutionnel**

- **DC n° 2018-765, 12 juin 2018,** constitutionnalité de la loi relative à la protection des données personnelles.
- **DC n° 2009-580, 10 juin 2009**, constitutionnalité de la loi favorisant la diffusion et la protection de la création sur internet, JurisData n° 2009-024431 ; JCP G 2009, 101, J.-Ph. Feldman.
- **DC n°99-419, 9 novembre 1999**, constitutionnalité de la loi relative au pacte civil de solidarité.
- **DC n° 99-416, 23 juillet 1999,** relative à la loi portant création d'une couverture maladie universelle, D. 2000. Somm. 265, obs. L. Marino, CCE 1999. Comm. 52, obs. R. Desgorces, RTD civ. 1999. 724, obs. N. Molfessis.
- **DC n° 92-316, 20 janvier 1993**, constitutionnalité du service central de prévention de la corruption et protection de la liberté individuelle en matière de fichiers informatiques, JORF n° 18 du 22 janvier 1993 p. 1118, Lucas A., Devèze J., Frayssinet J., note n° 100, n° 41, p. 28.
- **DC n° 81-132, 16 janvier 1982**, relative à la loi de nationalisation, Rec. Cons. const. 18 ; AJDA 1982. 202.
- **DC n° 73-51, 27 décembre 1973**, relative à la loi de finances pour 1974.
- **DC n° 71-44, 16 juillet 1971**, constitutionnalité de la loi complétant les dispositions des articles 5 et 7 de la loi du 1er juillet 1901 relative au contrat d'association.

**C. Décisions du Conseil d'État**

- **CE, ord. réf., 13 oct. 2020**, n° 444937, inédit, Lebon.
- **CE, 27 mars 2020**, n° 399922, Lebon.
- **CE, 10e et 9e sous-sections réunies, 12 mars 2014**, n° 353193, mentionné dans les tables du recueil Lebon.
- **CE, 24 août 2011**, n° 336382, Société HSBC Private Bank Suisse SA, mentionné dans les tables du recueil Lebon.
- **CE, 19 juill. 2010**, n° 317182, AJDA 2010, p. 1454, obs. de Montecler M.-C, Lebon.
- **CE, Ass.,10 juillet 1996**, n° 168702, 168734, 169631, 169951, Lebon.

**D. Décisions de cours d'appel**

- **CA Paris, 17 juin 2020**, RG n°18/23452.
- **CA Paris, Pôle 5, Ch. 11, 7 février 2020**, n° 18/03616.
- **CA Paris, 19 décembre 2018**, RG n° 17/03922
- **CA Paris, 16 mai 2018**, RG n° 17/11187.
- **CA Paris, Pôle 5, Ch. 2, 6 avril 2018**, n° 17/01312, Jamendo, Storever France et autres contre Sté Tapis Saint Maclou, SPRE et autres.
- **CA Paris, Pôle 6, Ch. 12, 18 janvier 2018**, n° 14/02884, EPIC Le Théâtre National de l'Opéra-comique de Paris contre URSSAF d'Île-de-France et AGESSA.
- **CA Bordeaux, Ch. civ. 1, 19 décembre 2017**, n° 16/7370, SCPP contre Productions 31 Distribution.
- **CA Rennes, 4 juillet 2017**, RG n°15/02244.
- **CA Toulouse, 28 juin 2017**, RG n°16/02093.

- **CA Paris, 21 juin 2017**, RG n°15/18784.
- **CA Paris, 30 mai 2017**, RG n°16/24129.
- **CA Paris, 22 février 2017**, RG n°16/17924.
- **CA Toulouse, 7 décembre 2016**, RG n°16/02774.
- **CA Aix-en-Provence, 3 novembre 2016**, RG n°14/13050.
- **CA Paris, 6 septembre 2016**, RG n°15/21026.
- **CA Paris, 18 mai 2016**, RG n°14/12584.
- **CA Paris, pôle 3, ch. 5, 13 avr. 2016**, n°10183000010.
- **CA Versailles, 31 mars 2016**, RG n°14/02978.
- **CA Versailles, 17 mars 2016**, RG n°14/02990.
- **CA Paris 12 février 2016**, n°15/08624.
- **CA Paris, 25 nov. 2015**, RG n°12/14513.
- **CA Paris, 1 juillet 2015**, RG n°13/19251.
- **CA Paris, 29 octobre 2014**, RG n°13/11059.
- **CA Paris, 10 octobre 2014**, n° 13/7387, Comm. Com. Élec. 2015, comm. 9, Caprioli E.
- **CA Paris, pôle 4, ch. 10, 5 février 2014**, nº 13/04833.
- **CA Paris, 11 septembre 2013**, RG n°11/17941.
- **CA Paris, 4 juillet 2013**, RG n°12/07651
- **CA Paris, 2e ch., pôle 5, 23 mars 2012**, RG n° 10/11168, Ryanair c/Opodo.
- **CA Paris, 26 avril 2006**, Comm. com. électr. 2006, comm. no 106, note Ch. Caron
- **CA Bordeaux, 5e ch., 9 novembre 2006**.
- **CA Paris, 4e ch., section A, 18 février 2004**.
- **CA Paris, 13e ch., section B, 12 avril 2022,** propr. ind. 2002, comm., nº 15, obs. Schmidt.
- **CA Paris, 4e ch., section A, 12 septembre 2001**, Tigest/Reed expositions France.
- **CA Aix-en-Provence, 1ère ch. B, 10 mai 2001**, D. 2002. Somm. comm. 2299, obs. A. Lepage.
- **CA Paris, 14e ch., 4 juillet 1997**, Expertises 1997, p.315.
- **CA Lyon, 24 février 1988**, PIBD 1988, III p. 225.
- **CA Paris, 15 mai 1970**, D. 1970. Jur. 466, concl. Cabannes.

**E. Décisions de tribunaux de grandes instances et de tribunaux correctionnels**

- **TGI Paris, 7 août 2018**, n° 14/07300
- **TGI Paris, 17e Ch., 15 novembre 2017**, X dite Cicciolina contre Société Y, Légipresse 2018, n° 357, p. 64 ; CCE 2018. Chron. 11, n° 3, obs. P. Tafforeau.
- **TGI Paris, 13e ch. Corr. 18 décembre 2014**, nº 12010064012, JurisData no 2014-032729; CCE 2015. Comm. 37, obs. É. A. Caprioli ; RSC 2015. 101, obs. J. Francillon.
- **TGI Nanterre, 30 novembre 2012**, UMP c/Oracle France, Expertises 2013, pp.358-360.
- **TGI Clermont-Ferrand, ch. Corr., 26 septembre 2011**, Sociétés X.. et Y.. c/ Mme Rose, Légalis.net, 6 oct. 2011 ; CCE 2012, comm. n° 36, note E. A. Caprioli.
- **TGI Paris, 24e ch. corr., 21 novembre 2014**, RG n° 10183000010, 13311000700, min. publ., iVentures Consulting a. c/Mme L. A.; CCE 2015, comm. 85, obs. É.-A. Caprioli.
- **TGI Paris, ord. réf., 16 sept. 2014,** M. et Mme X. et M. Y. c/Google France.
- **TGI Paris, 12e ch., 17 décembre 2010**, RLDI 2011/70, n° 2316.
- **TGI Paris, 17e ch civ., 24 novembre 2010**, CCE 2011, comm. 28, obs. Lepage
- **TGI Paris, 3e ch., 1ère section, 20 juin 2007**, www.legalis.net.
- **TGI Nanterre, 8 juin 2006**, RLDI 2007/25, nº 828, www.legalis.net.
- **TGI Paris 20 novembre 2000**, Yahoo c/Licra et UEJF, CCÉ 2000, no 132, obs. J.-C. Galloux – Paris, 17 mars 2004, CCÉ 2005, n° 72.

**F. Décisions de la Cour de justice de l'Union européenne**

- **CJUE, gde ch. 5 avril 2022**, affaire n° C-140/20, G.D. c/ Commissioner of An Garda Síochána et a..
- **CJUE, 10 décembre 2020**, affaire n° C-620/19, Land Nordrhein-Westfalen c/ D.H.T.
- **CJUE, 6 octobre 2020**, affaire n° C-623-17, Privacy International c/ Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service.
- **CJUE 6 octobre 2020**, affaire n° C-511/18, C-512/18 et C-520/18, , La Quadrature du Net e.a.
- **CJUE, 16 juillet 2020**, affaire n° C-311/18, Data Protection Commissioner c/ Maximillian Schrems et Facebook Ireland, SCHREMS 2, note Perray R., RLDI, n° 169, 2020. 35 ; note Martial-Braz N., JCP n° 41, 5 oct. 2020, p. 1116.
- **CJUE, 18 juin 2020**, affaire n° C-78/18, commission européenne c/ Hongrie.
- **CJUE, 24 septembre 2019**, affaire n° C-507/17, Google LLC c/ CNIL.
- **CJUE, 2 octobre 2018**, affaire n° C 207/16, Ministerio Fiscal.
- **CJUE, 5 juin 2018**, affaire n° C-210/16, Witschaftsakademie Schleswig-Holstein.
- **CJUE, 17 mai 2018,** affaire n° C-147/16, Karel de Grote.
- **CJUE, 21 février 2018**, affaire n° C-132/17, Peugeot Deutschland GmbH.
- **CJUE, 20 décembre 2017**, affaire n° C-434/16, Novak.
- **CJUE, 29 novembre 2017**, affaire n° C-265/16, VCAST Limited c/ RTI SpA.
- **CJUE, 6 septembre 2017**, affaire n° C-413/ 14, D. 2018. 865, obs. D. Ferrier.
- **CJUE, 19 octobre 2016**, affaire n° C-582/14, Breyer c/ Bundesrepublik Deutschland.
- **CJUE, 28 juillet 2016**, affaire n° C-191/15, Verein für Konsumenteninformation c./ Amazon EU Sàrl.
- **CJUE, 6 octobre 2015**, affaire n° C-362/14 Presse et Information Maximillian Schrems / Data Protection Commissione ; Schrems I, AJDA 2015. 2257, chron. Broussy E., Cassagnabère H. et Gänser C..
- **CJUE, 1er octobre 2015**, affaire n° C-230/14, Weltimmo.
- **CJUE, 11 décembre 2014**, affaire n° C-212/13, Affaire Ryneš.
- **CJUE, 13 mai 2014**, affaire n° C-131/12, Google Spain SL, Google Inc. c/ Agencia Española de Protección de Datos (AEPD) et Mario Costeja González.
- **CJUE, 24 novembre 2011**, affaire n° C-70/10, Scarlet Extended SA c/ Sté belge des auteurs, compositeurs et éditeurs, JurisData n° 2011-032131.
- **CJUE, 24 novembre 2011,** affaire n° C 468/10 et C 469/10, Asociación Nacional de Establecimientos Financieros de Crédito.
- **CJUE (grande chambre), 9 novembre 2010**, affaire n° C 92/09 Volker und Markus Schecke GbR et affaire n° C 93/09 Volker und Markus Schecke et Eifert c/ contre Land Hessen (affaires jointes).
- **CJUE, 4e ch., 16 juillet 2009**, affaire n° C-5/08, Infopaq International A/S c/Danske Dagblades Forening.
- **CJUE (grande chambre), 29 juin 2010**, affaire n° C-28/08, Commission c/ The Bavarian Lager Co. Ltd.
- **CJUE, 16 décembre 2008**, affaire n° C-73/07, Tietosuojavaltuutettu c. Satakunnan markkinapörssi oy et Satamedia oy.
- **CJUE, 11 janv. 2005**, affaire n° C-26/03 , Stadt Halle et RPL Recynclingpark Lochau GmbH, AJDA 2005. 898.
- **CJUE, 9 novembre 2004**, affaire n° C-203/02, The British Horseracing Board Ltd e.a. c/ William Hill Organization Ltd.
- **CJUE, 20 février 1979**, affaire n° 120/78, Rewe-Zentral AG contre Bundesmonopolverwaltung für Branntwein.

- **CJUE, 13 févr.1979**, affaire n° C-85/ 76, Hoffmann-La Roche c/Commission.
- **CJUE 14 décembre 1971**, affaire n° 43/71, Politi s.a.s. c/ ministère des finances de la République italienne.
- **CJUE 5 février 1963**, affaire n°26/62, NV Algemene Transport- en Expeditie Onderneming van Gend & Loos c/ Administration fiscale néerlandaise.

**G. Décisions de la Cour européenne des droits de l'homme**

- **CEDH, 28 juin 2007**, affaire n° 62540/00, Association for European Intégration and Human Rights and Ekimdzhiev c/ Bulgarie.
- **CEDH, 16 avril 2002**, affaire n° 37971/97, Sté Colas Est c/France
- **CEDH, 12 décembre 2001**, affaire n° 55207/99, Bancovic et autres c/ la Belgique, la République tchèque, le Danemark, la France, l'Allemagne, la Grèce, la Hongrie, l'Islande, l'Italie, le Luxembourg, les Pays-Bas, la Norvège, la Pologne, le Portugal, l'Espagne, la Turquie et le Royaume-Uni,
- **CEDH, 4 mai 2000,** affaire n° 14 566/05, Rotaru c/ Roumanie.
- **CEDH, 16 février 2000**, affaire n° 27 798/95, Amann c/Suisse.
- **CEDH, 16 décembre 1992**, affaire n° 13 710/88, Niemietz c/Allemagne, AJDA 1993. 105, chron. J.-F. Flauss ; D. 1993. 386, obs. J.-F. Renucci ; RFDA 1993.

**H. Décisions du Tribunal de l'Union européenne**

- **TPIUE, 22 novembre 2017**, affaire n° T-670/16, Digital Rights Ireland c/ Commission.
- **TPIUE, 7 juillet 2011**, affaire n° T-161/04, Gregorio Valero Jordana c/ Commission européenne, rec. 2011 II-00215.
- **TPIUE, 17 septembre 2007**, affaire n° T-201/04, Microsoft Corp. c/Commission des Communautés européennes, rec. 2007 II-03601, D. 2007. 2303, obs. E. Chevrier.

**I. décisions de juridiction étrangère**

- **Cour suprême des États-Unis, 17 avril 2018**, per curiam, United States petitioner vs/ Microsoft Corporation ; 584 US (2018) ; n° 17-2.
- **Tribunal britannique, 8 octobre 2018**, Lloyd v/ Google LLC [2018] EWHC 2599 (QB).
- **Cour d'appel britannique, 2 octobre 2019**, Lloyd v/ Google [2019] EWCA Civ 1599.
- **Cour constitutionnelle allemande, 15 décembre 1983**, BVerf GE 65, 1, Volkszahlung.

**J. Décisions de la Commissions européenne**

- Décision d'exécution (UE) 2016/1250 de la commission du 12 juillet 2016 conformément à la directive 95/46/ce du parlement européen et du conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE États-Unis, numéro C (2016) 4176.
- Décision de la Commission européenne numéro 200/520 du 26 juillet 2000 dans laquelle elle a considéré que le « Safe Harbor » ou autrement nommé « *le Bouclier de confidentialité* » offrait un niveau de protection adéquat des données transférées en provenance de l'Union européenne vers des entreprises établies aux États-Unis. Cet accord était effectif et applicable jusqu'à ce que la Cour de justice de l'Union européenne le suspende dans la décision du 6 octobre 2015 (aff. C-362/14).

# TABLE DES MATIÈRES

# INDEX ALPHABETIQUE

*(les chiffres renvoient aux numéros des pages)*

## *A*



## *B*



## *C*



## *D*

## *E*



## *G*



## *H*

## *I*



## *L*



## *M*



## *N*



## *O*



## *P*

## *R*



## *S*



## *T*



## *U*



## *V*