Contrat et données personnelles

Vincent Bertrand

THÈSE

Pour obtenir le grade de

Docteur

Délivré par

UNIVERSITE DE PERPIGNAN VIA DOMITIA

Préparée au sein de l'école doctorale

INTER-MED ED 544

Et de l'unité de recherche

CDED

Spécialité : **Droit privé**

Présentée par

Vincent BERTRAND

CONTRAT ET DONNEES PERSONNELLES

Soutenue le 19 novembre 2021 devant le jury composé de

M. Remy CABRILLAC, Pr, Université de Montpellier	Rapporteur
M. Christophe ALBIGES, Pr, Université de Montpellier	Rapporteur
M. Sylvain CHATRY, Pr, Université de Perpignan	Membre invité
M. Frédéric LECLERC, Pr, Université de Perpignan	Directeur de thèse
M. Emmanuel TERRIER, MCF, Université de Montpellier	Directeur de thèse

À mes parents pour leur amour et leur soutien inconditionnel

SOMMAIRE

DEUXIEME PARTIE : L'EXECUTION DU CONTRAT PORTANT SUR LES DONNEES PERSONNELLES

Titre 1 : L'exécution des contrats portant sur les données personnelles

Chapitre 1 : Les obligations en lien avec l'utilisation des données personnelles

Section 1 : La finalité des contrats portant sur l'utilisation de la donnée personnelle

Section 2 : Les modalités de l'utilisation de la donnée personnelle

Chapitre 2 : Les obligations liées à la protection de la donnée personnelle

Section 1 : Les données personnelles et les obligations de confidentialité

Section 2 : Les obligations de protection et de conservation des données personnelles

Titre 2 : L'inexécution des obligations portant sur les données personnelles

Chapitre 1 : Les sanctions au regard du contrat

Section 1 : Les sanctions liées à la responsabilité du contractant défaillant

Section 2 : Les sanctions frappant le contrat

Chapitre 2 : Les sanctions au regard du droit

Section 1 : La violation en lien avec des données personnelles au regard du droit civil

Section 2 : La violation en lien avec des données personnelles au regard du droit pénal et administratif

CONCLUSION GENERALE

** Voir la table des matières détaillée à la fin de l'ouvrage*

LISTE DES PRINCIPALES ABREVIATIONS

Actu.	Actualité
Aff.	Affaire
AJ.	Actualité juridique
AJCA.	Actualité juridique des contrats d'affaires
Al.	Alinéa
Anc.	Ancien
Art.	Article
BICC.	Bulletin d'information de la Cour de cassation
Bull.	Bulletin
Bull. civ.	Bulletin des arrêts des chambres civiles de la Cour de cassation
Bull. crim.	Bulletin des arrêts de la chambre criminelle de la Cour de cassation
c/	Contre
C. civ.	Code civil
C. com.	Code de commerce
C. pén.	Code pénal
C. rur.	Code rural et de la pêche maritime
C. sec. soc.	Code de la sécurité sociale
C. trav.	Code du travail
CA.	Cour d'appel
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. req.	Chambre des requêtes de la Cour de cassation
Cass. soc.	Chambre sociale de la Cour de cassation
CE.	Conseil d'État

CEDH.	Cour européenne des droits de l'homme
Cf.	*Confer*
CJCE	Cour de justice des Communautés européennes
CJUE	Cour de justice de l'Union européenne
CNIL.	Commission nationale de l'informatique et des libertés
Concl.	Conclusion
Cons. const.	Conseil constitutionnel
Consid.	Considérant
Conv. EDH	Convention européenne des droits de l'homme
CSP.	Code de la santé publique
Dalloz IP/IT	Revue Dalloz, droit de la propriété intellectuelle et du numérique
DDHC	Déclaration des droits de l'homme et du citoyen de 1789
Décr.	Décret
Dir.	Direction
DP.	Dalloz périodique
Dr.	Droit
DUDH	Déclaration universelle des droits de l'homme de 1948
Ed.	Edition
GAJC	Grands arrêts de la Jurisprudence civile
Gaz. Pal.	Gazette du palais
Ibid.	*Ibidem*
In.	Dans
Infra.	Ci-dessous
IP	Internet Protocol : identifiant d'un ordinateur

JCP.	Jurisclasseur périodique (Semaine juridique)
JORF.	Journal officiel de la République française
L.	Loi
Lebon	Recueil des arrêts du Conseil d'État
LGDJ.	Librairie générale de droit et de jurisprudence
LPA.	Les petites affiches
n.	Note
n°	Numéro
Obs.	Observation
op. cit.	*Opere citato*, cite précédemment
Ord.	Ordonnance
p.	Page
préc.	Précité
PUF.	Presses universitaires de France
Rapp.	Rapport
Rappr.	A rapprocher de
RDC.	Revue des contrats
RDSS	Revue de droit sanitaire et social
RGPD.	Règlement général sur la protection des données
RTD civ.	Revue trimestrielle de droit civil
RTD com.	Revue trimestrielle de droit commercial
RRJ.	Revue de recherche juridique et de droit prospectif

S.	Suivant
Sect.	Section
Somm.	Sommaire
Supra	Ci-dessus
T.	Tome
T. corr.	Tribunal correctionnel
TGI.	Tribunal de grande instance
UE.	Union européenne
URL	*Uniform resource locator*
V.	Voir
Vol.	Volume

INTRODUCTION

« *Le problème du contrat est de savoir sur quoi il se fonde* ».

André Glucksmann

1. Si le Code civil promulgué le 21 mars 1804 est une œuvre historique majeure[1], en avance sur son temps, il n'en reste pas moins que cet ouvrage doit, pour perdurer[2], s'adapter et ainsi connaitre, au fil du temps, quelques ajustements[3].

C'est pourquoi, à l'occasion du bicentenaire de ce modèle idéal de législation civile[4] que l'idée de rénover, si ce n'est de réformer, le droit des contrats était apparue nécessaire, et ce, pour plusieurs raisons[5].

Les dispositions du Code civil relatives au contrat avaient tout d'abord vieilli, ne reflétant plus la réalité du droit des obligations actuel[6]. Ensuite, ces mêmes dispositions n'étaient plus attractives, un rajeunissement de celles-ci s'imposait,

---

[1] *« La véritable Constitution de la France, c'est le Code civil »*, J. Carbonnier, *Le Code civil*, dans P. Nora (dir.), *Les lieux de mémoire*, t. 2, La Nation, Paris, Gallimard, 1986, p. 309.

[2] *« Ma vraie gloire, ce n'est pas d'avoir gagné quarante batailles : Waterloo effacera le souvenir de tant de victoires. Ce que rien n'effacera, ce qui vivra éternellement, c'est mon code civil ! »*, C-T. de Montholon, *Récits de la captivité de l'Empereur Napoléon à Sainte-Hélène*, Paris, 1847, t. I, p. 40.

[3] *« Qu'attendez-vous pour continuer la modernisation de votre code ? »*, P. Catala, *Présentation générale de l'avant-projet, Avant-projet de réforme du droit des obligations et de la prescription*, Rapport à Monsieur Pascal Clément, Garde des Sceaux, Ministre de la Justice, 22 Septembre 2005, p. 2.

[4] *« De ces deux noms accolés* (Portalis et Carbonnier) *s'exhalait une double certitude : que le Code de 1804 constituait toujours un modèle idéal de législation civile ; qu'il était possible de le rénover sans dégrader sa structure ni sa forme »*, *Ibid.*

[5] D. Mainguy, *Le nouveau droit francais des contrats, du régime général de la preuve et des obligations (après l'ordonnance du 10 février 2016),* UMR-CNRS 5815, Dynamiques du droit, 2016.

[6] B. Beignier, *Pour un nouveau Code civil*, Recueil Dalloz, 2019, p. 713 ; T. Revet, A propos de l'article de Bernard Beignier « Pour un nouveau Code civil », Recueil Dalloz, 2019, p. 1011 ; B. Beignier, Réponse à Thierry Revet (« Pour un nouveau Code civil »), Recueil Dalloz, 2019, p. 1408.

alors, afin de rendre le droit français plus compétitif[7]. Enfin, ces dernières n'avaient plus l'influence escomptée ni au plan européen, ni au plan mondial[8].

Si plusieurs avant-projets de réforme ont vu le jour entre 2005 et 2013 (avant-projet Catala[9], avant-projet Terré[10] et deux avants projets de la Chancellerie[11]), c'est la loi du 16 février 2015 qui a véritablement relancé la réforme relative « *à la modernisation et à la simplification du droit et des procédures dans les domaines de la justice et des affaires intérieures* »[12], autorisant ainsi le Gouvernement à réformer le droit des obligations par voie d'ordonnance, afin, notamment, « *de moderniser, de simplifier, d'améliorer la lisibilité et de renforcer l'accessibilité du droit commun des contrats* »[13].

Aux termes de cette loi, le Ministère de la Justice devait présenter une ordonnance de réforme avant le 17 février 2016. A cette fin, le Gouvernement a donc élaboré un « *projet d'ordonnance portant réforme du droit des contrats, du régime général de la preuve des obligations* »[14] publiée le 25 février 2015 et soumis à consultation publique.

Fort de ces nombreuses ébauches, et à la suite de cette consultation, l'Ordonnance portant réforme du droit des contrats, du régime général et de la preuve des

---

[7] *« Le Code civil n'est plus ni le reflet ni l'écrin du droit positif »*, D. Mazeaud, Présentation de la réforme du droit des contrats, Gazette du Palais, 2016, p. 15.

[8] R. Cabrillac, *Quel avenir pour le modèle juridique français dans le monde ?*, Economica, 2011 ; R. Cabrillac, *Un nouveau Code civil ?*, Recueil Dalloz, 2019, p. 2149.

[9] P. Catala, *Avant-projet de réforme du droit des obligations et de la prescription*, La Documentation française, 2006.

[10] Le projet est découpé en trois ouvrages : F. Terré, *Pour une réforme du droit des contrats*, Dalloz, 2009 ; F. Terré, *Pour une réforme du droit de la responsabilité civile*, Dalloz, 2011 ; *Pour une réforme du régime général des obligations*, Dalloz, 2013.

[11] Projet de réforme du régime des obligations et des quasi contrats (pour le droit des contrats, 2008 ; pour le régime général et la preuve des obligations, 2011).

[12] Loi n° 2015-177 du 16 février 2015 relative à la modernisation et à la simplification du droit et des procédures dans les domaines de la justice et des affaires intérieures.

[13] Art. 8, Loi n° 2015-177 du 16 février 2015 relative à la modernisation et à la simplification du droit et des procédures dans les domaines de la justice et des affaires intérieures.

[14] Projet d'ordonnance du 25 février 2015 portant réforme du droit des contrats, du régime général et de la preuve des obligations.

obligations[15] a été promulguée le 10 février 2016 et est entrée en vigueur le 1er octobre 2016. Quant à la loi de ratification[16], celle-ci a été promulguée le 20 avril 2018 et est entrée en vigueur le 1er octobre 2018, modifiant ainsi le droit des contrats issu de l'Ordonnance.

2. Les différentes étapes qui ont conduit à la réforme du droit des contrats de 2016 ayant été présentées, il convient désormais de s'intéresser à la notion même de « contrat ».

Entrant dans la catégorie des actes juridiques, comme étant l'élément central des sources volontaires des obligations, le contrat trouve son origine dans le formalisme du droit romain. Pour autant, c'est le principe du consensualisme qui en marque la caractéristique essentielle dans le Code civil, puisque sa définition en sera suffisamment large pour ne pas en limiter le champ.

Ainsi, et pour mémoire, l'ancien article 1101 du Code civil définissait le contrat comme « *une convention par laquelle une ou plusieurs personnes s'obligent, envers une ou plusieurs autres, à donner, à faire ou à ne pas faire quelque chose* »[17]. Cette définition traditionnelle du contrat était fortement critiquée par la doctrine[18]. Pour une majorité, le contrat étant seulement perçu comme une convention, il était donc regrettable de cantonner celui-ci à un rôle créateur d'obligations.

C'est la raison pour laquelle, le Code civil, depuis la récente réforme, définit le contrat à l'article 1101 nouveau comme « *un accord de volontés entre deux ou plusieurs personnes destinées à créer, modifier transmettre ou éteindre des*

---

[15] Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations (JORF n°0035 du 11 février 2016 texte n° 26).

[16] Loi n° 2018-287 du 20 avril 2018 ratifiant l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations (JORF n°0093 du 21 avril 2018 texte n° 1).

[17] C. civ., anc. art. 1101 *(Abrogé par Ord. nº 2016-131 du 10 févr. 2016, à compter du 1er oct. 2016)*.

[18] M. Latina, *Contrat : généralités, Notion de contrat*, Répertoire de droit civil, Mai 2017, n. 159 et 160 ; Y. Picod, *Obligations*, Répertoire de droit civil, Juin 2017, n. 37.

obligations »[19]. Au regard de ce texte, il apparait que le contrat repose désormais sur deux éléments. Pour qu'un contrat existe, il faut un accord de volonté (origine du contrat) conclu en vue de créer, modifier, transmettre ou éteindre des obligations (but du contrat).

C'est pourquoi, il semble désormais que tout acte juridique qui ne repose pas sur un accord de volonté et qui n'entraine pas d'effets juridiques relatifs à une obligation ne peut pas être qualifié de contrat.

La définition posée par l'article 1101 nouveau du Code civil se distingue de celle, autrefois, retenue par l'ancien article 1101 puisqu'elle exprime, désormais, une notion plus large et plus évasive. Aussi, la distinction entre contrat et convention est partiellement abandonnée. Si le contrat ne s'apparente plus à une simple convention, il est à présent défini comme toute forme d'accord dont le but est de créer, modifier, transmettre ou éteindre des obligations. Si certains auteurs reconnaissent que le nouveau texte permet de modifier, de scinder, la ligne de partage qui existait traditionnellement entre le contrat et la convention, ils regrettent, toutefois, que ce nouveau critère de distinction n'apparaisse pas distinctement[20]. Ces derniers sont, en effet, unanimes, la définition modernisée du contrat ne sera pas suffisante pour faire oublier l'effet essentiellement créateur de celui-ci. Ayant le mérite de proposer une solution, au problème précité, celle de fusionner les notions de convention et de contrat, il faut reconnaitre que l'analyse présentée est juste, pour autant elle ne doit pas amoindrir l'objectif premier de la réforme, celui d'apporter un nouveau souffle au droit des obligations, sans pour autant le bouleverser.

Il est donc clair que le droit actuel s'imprègne d'un renouveau, irrigué par l'Ordonnance du 10 février 2016[21], celui de moderniser le contrat y compris de l'adapter à des éléments sur lesquels celui-ci peut porter, à savoir des choses distinctes de celles que notre monde habituel connaissait telle que la chose

---

[19] C. civ., art. 1101 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

[20] S. Lequette, *La notion de contrat*, RTD. civ, 2018, p. 541.

[21] Loi n° 2015-177 du 16 février 2015, *préc.*

tangible matérielle. Ainsi, se posera la question de la faculté de pouvoir faire des données personnelles un élément du contrat.

Pour ce faire, il convient de garder à l'esprit que la validité du contrat est soumise à trois conditions, lesquelles sont précisées par l'article 1128 du Code civil : « *sont nécessaires à la validité d'un contrat : le consentement des parties, leur capacité de contracter et un contenu licite et certain* »[22].

Le cadre de l'étude sur les données personnelles et le contrat ne soulève pas de réelles difficultés quant à la notion de consentement, ni de manière directe à celle de la capacité. En revanche, la notion de contenu du contrat est-elle tout entière au cœur de la problématisation. Cette notion a connu un rajeunissement depuis la réforme du droit des obligations. S'il n'est plus question des traditionnelles notions d'objet et de cause, il faut désormais se référer uniquement à celle de contenu, ces deux notions ayant fusionné[23]. Ce changement terminologique ne peut, à lui seul, faire oublier les notions précédentes, puisque si les termes ont disparu, leur fonction demeure[24]. Il suffit pour s'en rendre compte de s'intéresser aux références qui déterminent la notion. En effet, si le contenu du contrat se doit d'être licite et certain, il est assurément encadré par le législateur de sorte qu'il « *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* »[25], comme le précise l'article 1162 du Code civil, s'appuyant lui-même sur les dispositions de l'article 6 du même Code.

3. Dès lors, et face à cet encadrement initial, qu'en est-il réellement du contenu du contrat ?

Cette problématique soulevée est d'autant plus pertinente que l'obligation, entendue au sens de « *but* » du contrat (confère l'article 1101 nouveau du Code

---

[22] C. civ., art. 1128 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

[23] F. Cohet, *Le contrat*, Droit en +, PUG, 2020.

[24] N. Dissaux, *Contrat : formation - Détermination des conditions*, Répertoire de droit civil, Avril 2017 (actualisation : Mars 2021), n. 158 et 159.

[25] C. civ., art. 1162 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

civil[26]), doit avoir, selon la loi (article 1163 du Code civil alinéa 1 et 2), « *pour objet une prestation présente ou future, possible et déterminée ou déterminable* »[27].

Ainsi, puisque l'existence d'un contrat est assujettie à certaines exigences et restrictions qui encadrent la notion, est-il important de savoir si celui-ci peut s'adapter aux différentes évolutions qui composent la société. En effet, de nos jours, les transformations économiques, sociales ou technologiques se multiplient et favorisent l'émergence de nouvelles considérations pour les personnes concernées. Naturellement, il convient de s'interroger sur ces avancées et leur place au sein du monde juridique. Une thématique, en particulier, semble retenir, sur elle, une attention particulière puisqu'elle permet de conjuguer la modernisation du droit des contrats et l'évolution technologique, d'autant plus que la confirmation d'un encadrement législatif de cette notion est intervenue quelques mois, seulement, après la réforme du droit des obligations.

Aussi convient-il de se demander, s'il est possible de confronter la détermination du but du contrat avec la notion de « données personnelles ». Pour ce faire, il apparait obligatoire de poser les bases et à ce sujet, afin de comprendre ce que sont les données personnelles, il convient méthodiquement de définir ces deux concepts séparément.

Si classiquement, une « donnée » est entendue, par l'Académie française, comme « *un fait ou un principe indiscuté, ou considéré comme tel, sur lequel se fonde un raisonnement ; constatation servant de base à un examen, une recherche, une découverte* »[28], la notion de « personnelle » se définit quant à elle, par le dictionnaire Larousse, comme ce « *qui appartient à quelqu'un, qui lui est propre* »[29].

---

[26] C. civ., art. 1101, *préc.*

[27] C. civ., art. 1163 *(Ord. nº 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

[28] URL : https://www.dictionnaire-academie.fr/article/A9D3040

[29] URL : https://www.larousse.fr/dictionnaires/francais/personnel/59814?q=personnelle#59449

Après avoir défini, de manière séparée, ces deux notions, il est à présent, toujours dans un souci de clarification, nécessaire de mettre en lumière ce que sont les « données personnelles ».

L'expression de « données à caractère personnel » ou communément appelée « données personnelles » se caractérise, en définitive, par le dictionnaire Larousse, comme « *les informations qui permettent d'identifier directement ou indirectement* » une personne[30]. Les données personnelles représentent également, de manière plus imagée, « *les éléments qui permettent de situer ou de préciser quelque chose (par exemple, les coordonnées d'une personne : son adresse)* »[31].

Juridiquement et historiquement, sous la présidence de Valéry Giscard d'Estaing, le droit spécial par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ou sobrement loi informatique et libertés[32], dans sa version initiale, en son article 2, déclarait pour définir les « données personnelles » telles qu'entendues de nos jours, « *sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale* »[33].

Dès les prémices, il est possible d'apercevoir le caractère novateur et protecteur de cette loi. En effet, si Jacques Thyraud, le sénateur à l'origine du Projet de loi relatif à l'informatique et aux libertés et Président de la Commission nationale de l'informatique et des libertés, ne cessait en 1978 de vanter les mérites de l'informatique, il était déjà pleinement conscient des dangers qu'impliquait cette invention. L'informatique, porteur de l'espoir d'une vie plus facile et meilleure, ne doit pas dominer les citoyens, mais être au service de ces derniers. Aussi, en

[30] URL : https://www.larousse.fr/infos/confidentialite

[31] URL : http://dictionnaire.sensagent.leparisien.fr/données%20personnelles/fr-fr/

[32] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (JORF du 7 janvier 1978 page 227).

[33] Art. 2, Loi n° 78-17 du 6 janvier 1978, *Ibid*.

véritable précurseur, comme c'est le cas en matière de droit de l'homme, la France entend par cette loi s'opposer aux appréhensions et conséquences fâcheuses de l'informatique pour la vie privée des personnes concernées. Il semble que, plus que d'essayer de maitriser l'informatique qui en était seulement, à cette époque, à ses balbutiements, la loi informatiques et libertés s'intéresse à garantir la sécurité de la vie privée des citoyens.

La définition précédemment présentée démontre également le souhait d'un champ élargi, afin de déterminer ladite notion et cela sans aucune restriction. Ce souci de généralité permet, d'une part, de justifier, une fois de plus, le coté avant-gardiste de la loi du 6 janvier 1978, mais également, d'autre part, d'englober dans la définition même des données personnelles des exemples à venir. En effet, dans les années 1980, les informations qui permettaient d'identifier une personne n'étaient, sensiblement, pas les mêmes qu'aujourd'hui.

Le développement de la société, mais aussi, et surtout celui de la technologie et, plus encore, celui de l'informatique entrainent la donnée personnelle dans une autre dimension. Pour preuve, il suffit, par exemple, de s'intéresser à une récente décision de la Cour de cassation, qui, au visa de l'article précité, « *vient de clore le débat sur la qualification de l'adresse IP*[34] »[35], en considérant qu'« *en statuant ainsi, alors 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, la cour d'appel a violé les textes susvisés* »[36].

Deux précédentes et importantes décisions étaient, auparavant, rendues, en ce sens, par la Cour de justice de l'Union européenne. En effet, cette dernière estimant, en 2011, que « *ces adresses* [comprendre – Les adresses IP des utilisateurs] *étant des données protégées à caractère personnel, car elles*

[34] Internet Protocol : identifiant d'un ordinateur.

[35] M. H, *L'adresse IP est une donnée personnelle*, Dalloz actualité, 8 décembre 2016.

[36] Cass. civ., 1ere, 3 nov. 2016, n° 15-22.595.

permettent l'identification précise desdits utilisateurs »[37], puis par une décision, du 19 octobre 2016[38], que « *Une adresse IP ''dynamique'' constitue une donnée à caractère personnel à l'égard de l'exploitant du site internet* »[39].

Si les trois affaires évoquées, ci-dessus, confirment, une fois encore, que la notion de donnée personnelle doit se définir de la manière la plus évasive possible, pour ne pas être restrictive, attention toutefois, celle-ci ne s'applique qu'aux seules « personnes physiques ». En effet, si, au même titre qu'une adresse IP, un fichier informatisé personnel ou privé constitue une donnée personnelle, cette affirmation ne l'est pas à propos d'un fichier « *se limitant à recenser des informations relatives à des personnes morales* »[40].
Si de plus amples approfondissements interviendrons, tout au long de cette étude, voilà, par ces quelques lignes de définition, un moyen permettant, d'abord, d'introduire la notion de donnée personnelle, puis, d'en établir le contexte.

4. Afin de contextualiser les différents propos, il parait opportun de proposer un développement historique et chronologique (avant et après la Loi informatiques et libertés de 1978) sur ce que sont les données personnelles dans leur généralité, permettant ainsi, plus tardivement, de mieux les intégrer et de mieux les comprendre au regard de leur connexité avec le droit des contrats.

En effet, si la Loi informatique et libertés de 1978 apparait comme une évolution précoce et majeure dans l'Histoire des données personnelles, donnant ainsi à cette notion une véritable importance comme le soulignera un auteur en indiquant que par cette loi « *la France marquait sa volonté de protéger les données personnelles face aux dangers que leur mise sur ordinateur fait courir à la vie privée* »[41], l'utilisation de celle-ci ne date pourtant pas d'hier. Déjà dans le passé, bien avant

---

[37] CJUE, 24 nov. 2011, aff. C-70/10.

[38] CJUE, 19 oct. 2916, aff. C-582/14.

[39] E. Autier, *CJUE : les adresses IP « dynamiques » sont des données personnelles au sens du droit de l'Union*, Dalloz actualité, 8 novembre 2016.

[40] G. Desgens-Pasanau, *La protection des données personnelles : Le RGPD et la loi française du 20 juin 2018*, LexisNexis, 4e édition, p. 15.

[41] A. Vitalis, *« Informatique et libertés » : une histoire de trente ans*, Hermès, La Revue, 2009/1, n°53, p. 137 à 143.

la Révolution française, la problématique entourant les données personnelles était de mise, alors que l'éclosion de ce qui allait devenir « l'informatique » était bien loin d'être imaginée et cela même par les plus illustres philosophes des Lumières…

En 1749, un gendarme dénommé Alexandre Guillauté suggérait, au roi de l'époque Louis XV, un projet, à savoir celui de la création d'un fichier des habitants de Paris[42].

Cette nécessité faisait spécifiquement écho aux nombreux mouvements de population existant durant l'Ancien régime ainsi qu'à l'émergence d'une nouvelle « police » adaptée aux besoins de société (préservation de la salubrité, maintien de l'ordre, lutte contre la mendicité et le vagabondage, contrôle des étrangers, méfiance du retour de la peste après celles des années 1720).

Fort de ce constat, courant du milieu du XVIII^{e} siècle, Guillauté proposait alors ce qui semble être comme l'un des premiers véritable « fichage »[43]. Si sa pensée pouvait, déjà à l'époque, paraitre radicale, elle avait pourtant le mérite d'être extrêmement bien maitrisée.

Pour réaliser son objectif, Alexandre Guillauté présentait un ouvrage[44] dans lequel il exposait ses méthodes, par exemple le fait de donner missions aux différents représentants de l'autorité.

S'il souhaitait moderniser l'institution de police et de ce fait diviser le pouvoir pour mieux l'utiliser[45], l'idée majeure de Guillauté était tout de même l'instauration d'un fichier de l'ensemble des habitants de Paris. Cette méthode de recensement, intrusive mais pour le moins ambitieuse, avait pour but de rassembler le maximum de renseignements et d'éléments concernant la population

---

[42] F. Mattatia, *RGPD et droit des données personnelles*, Éditions Eyrolles, 4^{e} édition, p.7.

[43] « *Action de recueillir et de stocker des renseignements sur des personnes, que ce soit sur des fiches cartonnées (traditionnellement) ou informatiquement* ».

[44] A. Guillauté, *Mémoire sur la réformation de la police en France : Soumis au roi en 1749*, Hermann.

[45] Cf. « *Divide et impera* » ou « *Diviser pour mieux régner* », maxime selon Philippe II de Macédoine.

parisienne en général, permettant ainsi un « quadrillage de l'espace » de la capitale et cela afin de mieux la contrôler.

Parmi toutes les minutieuses informations facilitant le travail de la police se trouvait notamment tout ce qui permettait utilement et simplement le « *repérage des personnes par l'administration* »[46].

Pour prouver son efficacité, il faut souligner que rien n'était épargné, ni laissé de côté, par le fichier de Guillauté lequel prenait exemple sur les registres de logeurs incluant par exemple, l'identité des individus, leurs professions, les revenus perçus et montants d'impositions acquittés, les dates d'entrée et sortie des occupants de l'immeuble ou encore la numérotation des appartements, escaliers et maisons[47]. Toutes ces déclarations étaient, bien entendu, à renouveler en cas de déménagement afin d'actualiser continuellement le fichage en question.

L'exemple du fichier « Guillauté », qui regroupe bon nombre d'informations relatives aux populations, ce qui sera perçu des décennies plus tard comme de la collecte de « données personnelles », s'inscrit dans un besoin de protection de la cité, de la population, ainsi que dans une perspective d'évolution et de modernisation de l'institution policière.

Toujours motivé par les mêmes problématiques, à savoir l'évolution de la police d'une part et l'évolution de la sécurité en général, une autre figure française est à l'origine d'un système d'identification internationalement utilisé (notamment beaucoup en Europe et aux États-Unis), là aussi à rapprocher des données personnelles actuelles.

---

[46] A. Guillauté, *Mémoire sur la réformation de la police en France : Soumis au roi en 1749*, *Op cit.*

[47] V. Milliot, *Réformer les polices urbaines au siècle des Lumières : le révélateur de la mobilité*, Crime, Histoire & Sociétés / Crime, History & Societies [En ligne], Vol. 10, n°1 | 2006, mis en ligne le 01 juin 2009, consulté le 02 mai 2019.
URL : http://journals.openedition.org/chs/195 ; DOI : 10.4000/chs.195

C'est à la fin du XIX[e] siècle et en la personne du criminologue français, Alphonse Bertillon[48], que le domaine scientifique criminel connait une de ses évolutions les plus prolifiques.

Ce dernier, après avoir travaillé au sein de la préfecture de police de Paris, s'intéresse à un phénomène qui représente à l'époque la moitié de l'univers carcéral, à savoir le cas particulier des « récidivistes » incorrigibles, c'est-à-dire ceux qui ne savent pas apprendre de leurs peines[49], assimilés à des asociaux qu'il faut éliminer[50].
Pour maitriser concrètement ce fait, en tant que petit-fils d'un démographe, fils d'un statisticien et anthropologue, Alphonse Bertillon développe, en véritable praticien, un système anthropométrique, appelé plus tard le « bertillonnage »[51], sur la base d'un constat simple.

En effet, il propose de mesurer plusieurs points précis du corps humain en regroupant ces informations dans un fichier, ce qui donnera naissance à une base de travail permettant d'identifier un criminel.

Mise au point des 1879, l'anthropométrie[52] (ou technique biométrique[53] de nos jours) se révélera très efficace puisque dès le 20 janvier 1883 le premier criminel récidiviste sera identifié et attrapé[54]. C'est donc avec Léon Durand, un voleur de

---

[48] C. Jalby, *La police technique et scientifique*, Pur édition, Collection Que sais-je, 2017.
URL : https://francearchives.fr/fr/commemo/recueil-2014/39094

[49] « *Cet être incorrigible, essentiellement mauvais, contre lequel la peine ne peut rien, est celui qui est promis à l'élimination* », JP. Allinne, M. Soula, *Les récidivistes : Représentations et traitements de la récidive (XIXe – XXIe siècle)*, Pur édition, p. 16.

[50] L. Mucchielli, *Criminologie, hygiénisme et eugénisme en France (1870 – 1914) : débats médicaux sur l'élimination des criminels réputés « incorrigibles »*, Revue d'histoire des sciences humaines, 2000, n°3, p. 57-88.

[51] « *Ce système d'identification reposait sur le relevé d'une vingtaine de mensurations du squelette et de la photographie de face et de côté »,* URL : https://www.senat.fr/rap/r04-439/r04-4394.html#fn46

[52] « *Née au milieu du XIXème siècle, l'anthropologie est la science de l'homme. L'une de ses branches, l'anthropologie physique ou anthropométrie, étudie les caractères anatomiques et biologiques de l'homme »,* URL : https://www.senat.fr/rap/r04-439/r04-4394.html#fn44

[53] « *La biométrie est, au sens étymologique, la mesure des choses vivantes, par un abus de langage, elle désigne l'ensemble des technologies de reconnaissance physique ou biologique des individus* », URL : https://www.senat.fr/rap/r04-439/r04-4394.html

[54] G. Macé, *Le Service de la Sureté par son ancien chef*, Paris, Charpentier, 1884, p. 376 sv.

bouteille mesuré et analysé par Bertillon, que le « bertillonnage » sera testé et approuvé.

Fort de cette réussite et de ce succès[55], le système sera importé et utilisé partout dans le monde, notamment en Europe et aux États-Unis, le journal « New York Times » décrivant, plus tard, son inventeur comme « *un des policiers les plus illustres du XIX^e siècle* »[56].

Si ces différents fichages (tant celui dit de Guillauté, que celui de Bertillon), qui paraissent pourtant « radicaux » du fait de leur pointilleuse intrusion chez les personnes sujettes, semblent bienvenu, il est dans l'Histoire des collectes d'informations relatives aux populations (donc aux données personnelles) qui comportent des aspects plus négatifs tant le but poursuivi qui les animent se relève être beaucoup plus sombre.

Aussi, voilà venu le moment d'introduire un passage relatif à l'esprit « 1942 ». Si ce titre, n'a nul besoin d'explication, c'est parce qu'il évoque l'une des périodes modernes les plus sombres de l'Histoire française.

C'est désormais à l'aune du milieu de la Seconde Guerre mondiale et sous le prisme des données personnelles qu'il convient de s'intéresser. Il sera, en effet, ici question de la constitution de fichiers, donc de collectes de données personnelles, sous le triste régime de Vichy. Le développement, à venir, sera bien entendu à confronter avec celui précédemment évoqué, tous deux étant nécessaires pour comprendre l'émergence des données personnelles.

Avant cela, il convient de faire un bref rappel de la situation de la France au moment de l'instauration du régime emmené par le Maréchal Philippe Pétain.

---

[55] P. Piazza, *Aux origines de la police scientifique – Alphonse Bertillon, précurseur de la science du crime*, Karthala édition, Collection Homme et sociétés, 2011, p. 322.

[56] URL : https://www.nytimes.com/1914/02/15/archives/alphonse-bertillon.html

Au milieu de la Seconde Guerre mondiale et fort de ses nombreuses victoires et invasions à l'Est (notamment en Pologne), le gouvernement du III^e *Reich* allemand remporte la Bataille de France[57] et continue son ascension vers les Pays-Bas, le Luxembourg et la Belgique.

Après avoir signé la convention d'Armistice[58] le 22 juin 1940 à Compiègne, manifestation de la capitulation de l'armée française, le territoire français se retrouve scindé en deux zones par l'armée allemande (une zone libre et une zone occupée). Découpé et occupé, le pays est affaibli, tant au plan politique que militaire, sa déroute amenant la fin de la République pour l'émergence d'une nouvelle institution, le régime de « Vichy ».

Sur la question des données personnelles, ledit régime, dont la période s'étend du 10 juillet 1940 (vote des pleins pouvoirs au Maréchal Pétain à l'Assemblée nationale) au 20 aout 1944 (départ du Maréchal Pétain)[59], ne fait que reprendre ce qui existait déjà, par exemple les deux systèmes de fichages précédemment énoncés[60], cependant le but poursuivi y est dorénavant différent, pour ne pas dire dramatique. Quoi qu'il en soit, il reste cependant important et nécessaire de traiter des différentes configurations de l'utilisation des données personnelles, même les plus extrêmes, afin de mieux les cerner.

En apparence, si les techniques utilisées par le régime de Vichy ne semblent pas si éloignées de celles déjà susvisées[61], le recours aux données personnelles y est, pourtant, plus intrusif que jamais, notamment en ce qu'il catégorise certaines populations, bien plus que les autres.

---

[57] La Bataille de France est une campagne menée par l'armée allemande du III^e *Reich* débutée le 10 mai 1940 et se terminant « *le 22 juin par une capitulation inconditionnelle de l'armée française à Compiègne* », URL : https://carlpepin.com/2010/09/07/la-bataille-de-france-1940/

[58] « *Le 22 juin, l'armistice est signé. Il aboutit au morcellement du pays en zones et au maintien d'un gouvernement français sous l'autorité du Maréchal. L'armistice est le véritable acte de naissance du nouveau régime* », D. Peschanski, *Vichy 1940-1944 : contrôle et exclusion*, Edition complexes, p. 19.

[59] M-O. Baruch, *Le régime de Vichy 1940-1944*, Paris, Tallandier, 2017.

[60] *Cf. Supra, fichier « Guillauté » et « Bertillonnage ».*

[61] *Ibid.*

Il est pertinent de s'intéresser, de plus près, aux mécanismes mis en place par le régime de Vichy et par là de mettre en lumière l'utilisation des données personnelles dans sa forme la plus négative qui soit.

C'est en effet, sous l'occupation et la pression allemande que la France du Maréchal Pétain dû développer de nouveaux moyens, toujours de plus en plus contraignants, pour contrôler les populations dans le but de ce qui sera un des moteurs de la « collaboration »[62], à savoir l'identification de la population juive.

Dés 1921, le préfet de police obligeait la population parisienne à se munir d'une « carte d'identité de français »[63], mais ce n'est qu'en septembre 1940, sous l'impulsion de l'armée allemande, que cette carte s'impose à tout individu français âgé de plus de 16 ans, cette même armée qui avait déjà façonné un mois plus tôt le recensement de tout juif vivant sur le territoire[64].

Si le fichage avait, à l'époque, pour but de maitriser et d'épurer les criminels, l'utilisation qui en est faite ici est tout autre puisqu'il s'agit purement et simplement d'exclure un certain type de la population mondiale en fonction de sa race, son origine, son ethnie ou encore son appartenance religieuse.

La méthode était simple, l'administration adjugeait à chaque individu une carte d'identité similaire en sa forme, toutefois la mention « juif » y était apposée pour certains. Si le racisme est présent dans l'Histoire depuis des milliers d'années, il semble que ce procédé, dans lequel une administration, un régime, un pays, participe activement et directement à discriminer, n'a pas existé depuis la fin de l'esclavage en France, soit plus d'un siècle plus tôt.

---

62 « *La fortune politique de la collaboration nait, on le sait, le 24 octobre 1940 de la poignée de main du maréchal Pétain, chef du nouvel État français né de la défaite, et du chancelier vainqueur Adolf Hitler* », P. Ory, *Les collaborateurs : 1940-1945*, Éditions du Seuil, p.36.

63 P. Piazza, *Histoire de la carte nationale d'identité*, Odile Jacob, 2004.
P. Piazza, *Septembre 1921 : la première « carte d'identité de Français » et ses enjeux*, Genèses, 01 Mars 2004, Vol. 54(1), pp. 76-89.

64 C. Halpern, *Une identité nationale en papier, Identité(s) : L'individu, le groupe, la société*, Éditions Sciences Humaines, Collection Synthèse, 2016.

L'Histoire démontre que la collecte d'information, ou données personnelles, est un mécanisme qui s'il ne parait pas si grave en substance peu, en profondeur, devenir d'une violence inouïe.

Le simple fait d'apposer une mention sur un papier, une carte, un fichier, tel que par exemple l'inscription du simple mot « juif » a pu causer des conséquences dramatiques.

C'est en effet à cause de cette technique du recensement que le III^e *Reich* a pu mener à bien son projet et assouvir sa folle mission, à savoir le génocide de populations afin de promouvoir la soi-disant « race aryenne ».

5. Si la Seconde Guerre mondiale marque un tournant majeur dans l'Histoire des données personnelles, développant ainsi cette notion et son utilisation, il existe, dès le début des années 1970, une révolution technologique considérable changeant l'approche de celles-ci permettant de les faire évoluer jusqu'à ce qu'elles deviennent ce qu'elles sont aujourd'hui.

C'est à partir de cette année-là, début XX^e siècle, que la protection autour des données personnelles émerge considérablement, dans un contexte favorable causé par les nombreux progrès technologiques.

Si la date du 1^er janvier 1970 est choisie pour représenter symboliquement dans l'univers informatique l'origine du temps, appelé aussi *timestamp* [65], cela démontre bien que cette période marque l'avènement de l'informatique, en perpétuelle croissance, et de tout ce que cela fait peut rejaillir sur les notions voisines.

[65] Le *timestamp* est un outil de conversion ou mesure de temps, utilisé en informatique, désignant le nombre de seconde écoule depuis une heure précise à savoir le 1^er Janvier 1970 à minuit.

C'est donc réellement dans les années 1970 que la « révolution numérique »[66] est en marche et cela dans tous les domaines, les données personnelles étant directement affectées par cette nouvelle « mode ».

D'un système de fichage archaïque sur un bout de papier, sorte de simple recensement, les données personnelles se voient désormais englouties par les outils informatiques et numériques. Toutes ces innovations amenant, de par leur complexité et leur puissance, à un accroissement massif de récolte des données et donc, c'est le revers de la médaille, à des dérives et violations de toutes les informations personnelles des individus.

Si d'un côté, la technologie ne cesse de se développer, ce qui peut faire craindre pour la sécurité des données personnelles (pour leur récolte et/ou leur utilisation), fort heureusement, de l'autre, la loi et le droit sont présent pour apporter un cadre. Ainsi, l'instauration de régimes juridiques permet d'éviter certaines dérives, notamment en matière de données personnelles, lesquelles sont de par leur nature même, tel que plusieurs fois évoquées, des données ultrasensibles.

Il est maintenant démontré que, tout au long de l'Histoire, la donnée personnelle est une donnée sensible, propre à chacun et que ceux qui l'utilisent ne peuvent en user comme bon leur semble, au risque de commettre des actes aux conséquences aussi néfastes que désastreuses.

6. Durant les différentes périodes de l'Histoire, la donnée personnelle est perçue, sous différents angles et selon le point de vue comme, une donnée parfois nécessaire pour détenir la main mise sur une population et en assurer la paix (sociale, criminelle), tantôt vitale, notamment pour un gouvernement (en temps de crise ou de guerre) et toujours rare et personnel pour les individus qui en sont dépossédés.

C'est fort de ce constat qu'il convient, désormais, de s'intéresser au cadre législatif existant depuis l'entrée en vigueur de la loi informatique et libertés, loi

[66] E. Scherer, *La révolution numérique : Glossaire*, Dalloz, 2009.

dont l'application représente, dès 1978, un tournant décisif pour les personnes concernées et leurs données personnelles. En effet, ce texte audacieux s'impose, peu de temps après l'éclosion d'internet, comme un repère et un garant pour la protection des données personnelles et pour la vie privée de leurs propriétaires.

Aussi, c'est pourquoi, il parait, avant tout, nécessaire ou plutôt impératif, puisque l'approche historique le permet, de développer cette notion clé pour les données personnelles, soit le principe de « vie privée ».

La naissance de ce concept, qui existe malgré lui (car sans véritable cadre), est tacitement présente depuis tout temps, depuis que l'Homme l'est aussi.

En effet, énoncer que chacun a droit au respect de sa vie privée est un postulat incontestable. Mais s'il est de nos jours aisé d'affirmer une telle notion, la reconnaissance de celle-ci est, étonnamment, « *récente et imprécise* »[67].

C'est d'ailleurs, seulement, par une loi du mois de Juillet 1970[68] que fut intégrée dans le Code civil, à l'article 9, la disposition pionnière suivante à savoir : « *chacun a droit au respect de sa vie privée* »[69].

Si le concept de vie privée innove par sa modernité, il n'était pas pour autant inconnu de l'Histoire. Déjà en 1789, la Déclaration des droits de l'Homme et du citoyen reconnaissait la notion de « sureté »[70] comme un droit fondamental et s'imposait comme « *garantie offerte contre les arrestations et les peines*

---

[67] F. Mattatia, *RGPD et droit des données personnelles*, *Op cit*, p.8.

[68] Loi n° 70-643 du 10 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens.

[69] C. civ., art. 9 (L. n°70-643 du 17 juill. 1970).

[70] « *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 sureté et la résistance à l'oppression* », Art. 2, DDHC 1789.
« *Nul homme ne peut être accusé, arrêté ni détenu que dans les cas déterminés par la loi, et selon les formes qu'elle a prescrites. Ceux qui sollicitent, expédient, exécutent ou font exécuter des ordres arbitraires, doivent être punis ; mais tout citoyen appelé ou saisi en vertu de la loi doit obéir à l'instant : il se rend coupable par la résistance* », Art. 7, DDHC.

arbitraires »[71] ou en d'autres termes une « *protection pour les individus contre les abus de pouvoir et violence* »[72]. Aussi, si la finalité n'était pas exactement la même pour ces notions, le but poursuivi par ces deux principes était identique, à savoir la protection suprême des individus. Véritable ancêtre, la notion de sureté allait connaitre quelques modifications et précisions jusqu'à définitivement évoluer et devenir le concept de vie privée tel qu'il est aujourd'hui.

En effet, affirmée par la Déclaration universelle des droits de l'homme (DUDH) des nations unies de 1948[73], la protection de la vie privée[74] se voit véritablement consacrée en droit français à la fin du XX^{e} siècle lorsque le Conseil Constitutionnel rend, en 1999, une décision[75] à propos d'une loi pour l'instauration d'une couverture maladie universelle rattachant ainsi le droit au respect de la vie privée de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 précédemment évoquée[76].

Si le concept de « vie privée » est si important en matière de données personnelles c'est parce que l'utilisation de ces dernières est conjuguée et démultipliée par l'emballement inertiel, sans précédent, causé par l'évolution informatique et technologique.

A ce sujet, pour éclairer les propos ci-dessus, il convient d'avoir à l'esprit le reportage du journaliste Philippe Boucher qui, en ce jour du 21 mars 1974,

---

71 URL : http://espacehgfauthoux.e-monsite.com/medias/files/lecon-n-5-la-surete-un-droit-de-l-homme.pdf

72 F. Mattatia, *RGPD et droit des données personnelles*, *Op cit*, p.8.

73 URL : https://www.un.org/fr/universal-declaration-human-rights/

74 « *Nul ne sera l'objet d'immixtions arbitraire dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* », Art 12, DUDH 1948.

75 « *Considérant qu'aux termes de l'article 2 de la Déclaration des droits de l'homme et du citoyen : « 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. » ; que la liberté proclamée par cet article implique le respect de la vie privée* », Cons. const., 23 juill. 1999, n° 99-416 DC, cons. 45.

76 V. Mazeaud, *Nouveaux cahiers du conseil constitutionnel n°48 (Dossier : Vie privée)*, Juin 2015, p. 7-20.

publiera dans le quotidien « Le Monde » l'article suivant : « SAFARI ou la chasse aux français »[77].

Cette chronique fait référence à un projet qui émerge depuis le début des années 1970, dont l'acronyme est SAFARI pour Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus, lequel est destiné à définir chaque français par un identifiant. Ce système inquiétant vise à croiser les fichiers existant en vue, ni plus ni moins, de ficher les français, et ce, sans soumettre le projet au Parlement…

L'émoi provoqué par ces révélations[78], au sein de l'opinion publique, conduira ou plutôt contraindra le gouvernement français à adopter[79] la loi informatique et libertés en 1978[80].

Plus loin encore, puisque le projet SAFARI faisait craindre certains danger liés à l'utilisation de l'informatique, notamment un fichage général de population, obligeant alors le gouvernement et le président de l'époque, en la personne de Valéry Giscard d'Estaing, à créer une commission afin qu'elle propose des mesures tendant à garantir que le développement de l'informatique se réalisera dans le respect de la vie privée, des libertés individuelles et des libertés publiques.

La commission informatique et libertés, présidée à ce moment-là par Bernard Chenot s'attela alors à la création de la première autorité indépendante administrative : la Commission Nationale de l'Informatique et des Libertés, dit la CNIL était donc née !

---

[77] P. Boucher, *« SAFARI » ou la chasse aux Français*, Le Monde, 21 mars 1974, p. 9.
URL : https://www.cnil.fr/sites/default/files/atoms/files/le_monde_0.pdf
URL : https://www.lemonde.fr/archives/article/1974/03/21/une-division-de-l-informatique-est-creee-a-la-chancellerie-safari-ou-la-chasse-aux-francais_3086610_1819218.html?xtmc=safari&xtcr=1274

[78] G. Desgens-Pasanau, *La protection des données à caractère personnel : La loi « informatique et libertés »,* LexisNexis, Carré droit, p. 3.

[79] « *Trois événements ont plus particulièrement contribué à cette mobilisation des esprits. Ce fut tout d'abord un article retentissant du Conseiller d'État Philippe Boucher (…). Cet article fut en grande partie à l'origine de la prise de conscience, par les politiques, des enjeux de l'informatisation au regard des libertés individuelles* », L. Joinet, Expert indépendant auprès de la Commission des droits de l'homme de l'ONU, Audition à la Commission nationale de l'Informatique et des Libertés, 8 mars 2005.

[80] Loi n° 78-17 du 6 janvier 1978, *préc.*

L'intérêt d'un tel organisme, qui plus est indépendant, avait, principalement, pour vocation de protéger la population contre les méthodes de renseignement du gouvernement, à son égard, ce qu'un auteur résume, par ces mots « *A l'époque, le risque ressenti comme majeur résidait dans les fichiers que seul le gouvernement et quelques entreprises pouvaient s'offrir* »[81].

Cette pensée était, déjà celle, en son temps, partagée par le procureur général de la Cour de cassation, Adolphe Touffait, qui alertait l'Académie des sciences morales et politiques en annonçant que « *La dynamique du système qui tend à la centralisation des fichiers risque de porter gravement atteinte aux libertés, et même à l'équilibre des pouvoirs politiques* »[82].

Si, autrefois, seul le gouvernement ou bien quelques entreprises avaient les moyens et la capacité d'intercepter des données personnelles, la situation est bien différente aujourd'hui puisqu'il est beaucoup plus facile de détenir une information sur quelqu'un, sans se limiter à une seule personne, ni même une seule information.

Voilà pourquoi, grâce à son statut particulier d'autorité administrative indépendante, la Commission nationale de l'informatiques et des libertés, organisme public ayant vocation à agir au nom de l'État sans pour autant être placé sous l'autorité du gouvernement, peut alerter, conseiller et informer tous les publics en veillant à ce que l'informatique se cantonne à être au service du citoyen sans porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni même aux libertés individuelle publiques[83]. Pour ce faire, ladite commission dispose d'un véritable pouvoir de contrôle et de sanction dans l'objectif de protéger les données personnelles contenues dans les fichiers et traitements informatiques ou papier, aussi bien publics que privés[84].

Une dernière remarque, à propos de l'article de Philippe Boucher, permet d'apprécier, également, non sans humour, l'existence de l'évolution technologique et par là le besoin et les enjeux concernant la collecte de données

[81] F. Mattatia, *RGPD et droit des données personnelles*, *Op cit*, p.11.

[82] A. Touffait, Communication à l'Académie des sciences morales et politiques, 9 avril 1973.

[83] URL : https://www.cnil.fr/fr/cnil-direct/question/la-cnil-cest-quoi

[84] *Ibid.*

personnelles, celui-ci précisant que « *Pour mesurer les progrès effectués depuis cette époque, on notera que l'auteur soulignait l'effrayante capacité de stockage de l'ordinateur du ministère de l'intérieur en 1974 : une mémoire de 2 Go… »*[85]. Pour les moins expérimentés, il faut savoir qu'à l'heure actuelle, n'importe quelle clef USB classique est pourvue d'une capacité minimale de stockage équivalente à 2 Go…! L'évolution technologique constatée permet de prendre conscience et de mesurer les dangers qui existent à l'heure actuelle et qui existeront dans le futur pour la protection des données personnelles. La vitesse de traitements des données personnelles est désormais si rapide que ces derniers sont réalisés quasiment en instantané et la quantité de stockage est de son côté infinie. La capacité technologique des outils informatiques est, pour l'heure, si avancée qu'il parait inévitable, afin d'éviter certaines dérives, de se munir d'arguments en faveur de la protection des données personnelles et des personnes concernées comme a pu l'incarner la loi informatique et libertés de 1978.

7. Il convient, à présent, de fournir quelques explications sur une pensée naïve et choquante démontrant l'état dans lequel se trouvait le monde, quelques années plus tard, et par là, l'urgence de l'arrivée tant attendue d'un véritable contrôle relatif à la protection des « données personnelles ». Avant cela, voici les propos en question : « *If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place* »[86]. Cette sortie médiatique, remarquée, a pu paraitre étonnante et ainsi avoir des conséquences.

Par ces quelques mots, le Président directeur général de la firme « Google » avait affirmé sa position quant à l'absence manifeste, pour lui, d'une quelconque vie privée. Partant de ces déclarations, le constat ne peut être que des plus clair. Si une firme aussi puissante que le géant « Google », entreprise au rayonnement mondial, bafoue la vie privée et par là les « données personnelles » de millions d'utilisateurs, la crise était proche. La multiplication des atteintes aux données personnelles, toujours réelles et présentes, poussait Philippe Boucher en 2011 à

---

[85] F. Mattatia, *RGPD et droit des données personnelles*, *Op cit*, p.11.

[86] « *Si vous faites quelque chose que personne ne doit savoir, peut-être devriez-vous commencer par ne pas le faire* », URL : https://www.eff.org/fr/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy

dresser un constat amer sur une éventuelle sortie de crise pour l'avenir et le bien de ces dernières, lui qui émettait des doutes sur la crédibilité d'un quelconque contrôle[87].

Peu de temps après, ,durant l'année 2013, le scandale provoqué par l'affaire « Snowden », nom du lanceur d'alerte à l'origine des révélations, fait figure d'élément déclencheur et de prise de conscience pour s'assurer, de la manière la plus pérenne qu'il soit, de la protection des données. Cette affaire dont « *l'onde de choc provoquée par la plus importante fuite de documents de l'histoire des services de renseignements américains se mesure encore aujourd'hui* »[88] expose au grand public certaines pratiques de collectes de renseignements utilisées par les services secrets notamment américains et britanniques. Ainsi, Edward Snowden, ancien consultant de la NSA (National Security Agency), contribue à dévoiler, au grand jour, que premièrement « *les gouvernements, y compris démocratiques, exercent une surveillance de masse sur leurs propres citoyens* »[89], qu'ensuite « *les grandes entreprises numériques, lorsqu'elles n'étaient pas victimes des agences de renseignement, en étaient complices* »[90] et enfin, plus grave encore, que n'importe quel individu participe, également, sans le savoir, à la collecte massive de données causée par les interactions numériques, quotidiennes.

Voilà pourquoi, le monde des « données personnelles » s'entoure d'une volonté grandissante d'un encadrement de dimension international, régional, et qui au plan européen donnera lieu à la création du fameux règlement général sur la

---

87 « *Dans cette situation, il ne me parait pas excessif de dire que la CNIL […] a atteint les limites de son pouvoir. De sorte que les craintes nées avec SAFARI ont de quoi faire sourire aujourd'hui. Mais un sourire en forme de grimace* », P. Boucher, cité par le site idh-toulon.net, 2 avril 2011.

88 M. Untersinger, *Ce que les « révélations Snowden » ont changé depuis 2013*, Le Monde, 13 septembre 2019.

89 B. Puybareau, *Les révélations d'Edward Snowden : de l'indignation à la légalisation des pratiques de surveillance*, Institut Open Diplomacy, 4 juin 2020.

90 N. Barreiro, *Affaire Snowden : révélations, demande d'asile… ce qu'il faut savoir*, RTL, 16 septembre 2019.

protection des données, alors transposé par la suite au droit français le 20 juin 2018[91].

A ce propos, la contribution de l'affaire « Snowden » est soulignée et remarquée par le député français, Cédric Villani, qui, se réjouissant de l'arrivée d'un règlement renforçant le droit des individus sur l'utilisation de leurs données personnelles, déclarait cet hommage, à savoir que « *Ce RGPD, il y a de quoi en être fier au niveau européen, mais il faut avoir conscience qu'il a été adapté sous la pression et par la peur, la peur suscitée par l'affaire Snowden aux États-Unis. Sans l'héroïsme d'Edward Snowden, il est possible que nous n'aurions pas aujourd'hui cet outil législatif protecteur* »[92].

Si le règlement européen ne peut pas, éradiquer, tous seul, l'utilisation malhonnête et le traitement déloyal des données personnelles, il peut, toutefois, apporter un cadre et surtout faire changer les mentalités[93]. Que ce soit du côté des individus ou de ceux qui se servent des données personnelles, le règlement démontre en quoi ces données sont sensibles et comment les appréhender et cela dans le plus grand respect de tous.

C'est pourquoi, en son article 4, relatif aux définitions, ledit règlement présente les données à caractère personnel, communément les « données personnelles », comme « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée) »* et le texte ajoute *« est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence ce à un identifiant, tel qu'un nom, un numéro d'identification, des données de*

---

[91] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (JORF n°0141 du 21 juin 2018 texte n° 1).

[92] Propos recueillis le 12 juin à Lyon par L. Rigier et V. Benais.
URL : https://france3-regions.francetvinfo.fr/auvergne-rhone-alpes/rhone/lyon/lyon-cedric-villani-eclaire-notre-lanterne-intelligence-artificielle-1494023.html

[93] « *Les gens disent que rien n'a changé parce qu'il y a encore de la surveillance de masse. Mais ce n'est pas comme ça que vous mesurez le changement. Tout a changé [depuis 2013]. Le gouvernement et les entreprises privées tiraient profit de notre ignorance. Mais désormais, nous savons. Les gens sont conscients. Nous sommes encore impuissants, mais nous essayons. Les révélations ont équilibré le combat. Les gouvernements et les entreprises sont dans le jeu depuis longtemps et nous commençons tout juste* », E. MacAskill and Alex Hern, Edward Snowden : *'The people are still powerless, but now they're aware'*, The Guardian, Interview, 4 juin 2018.

localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, psychologique, génétique, psychique, économique, culturelle ou sociale »[94].

8. Après avoir introduit le sujet, il convient dorénavant de présenter, en détail, le règlement général sur la protection des données personnelles, son contenu, sa philosophie, ainsi que ses objectifs.

Pour reprendre, Alexis Baumann, spécialiste en la matière, le règlement général sur la protection des données, ou communément nommé RGPD (en anglais : « GDPR » pour « *General Data Protection Regulation* »), est 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[95].

Il représente de l'espoir pour la vie privée des personnes concernées, puisqu'il a pour principale mission d'encadrer législativement tous traitements de données personnelles sur le territoire de l'Union européenne. Adoptées définitivement par le Parlement européen le 14 avril 2016, les dispositions propres à ce dernier (*cf. RGPD*) sont entrées en vigueur le 25 mai 2016 et sont applicables, au sein des 28 États membres de l'Union européenne, depuis le 25 mai 2018[96].

Ce même règlement a pour but précis, selon la Commission nationale de l'informatique et des libertés de « *renforcer le contrôle par les citoyens de l'utilisation qui peut être fait des données les concernant* », et permet également, « *d'harmoniser les règles en Europe en offrant un cadre juridique unique aux professionnels* »[97]. Pour réaliser cet objectif, ce dernier s'articule autour de six

[94] RGPD art. 4, Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

[95] URL : https://www.dictionnaire-juridique.com/definition/rgpd.php

[96] Communication de la Commission au Parlement européen et au Conseil, Une meilleure protection et de nouvelles perspectives, Orientation de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018.
URL : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52018DC0043&from=FR

[97] URL : https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on

grands axes principaux : la transparence des traitements, le consentement explicite, la limitation de la conservation des données, la confidentialité et la sécurité des données, la co-responsabilité entre le responsable du traitement et de ses sous-traitants et enfin le principe d'*accountability* qui impose au responsable du traitement de prouver sa conformité.

En France, ce texte s'inscrit dans la continuité de la loi relative à l'informatique, aux fichiers et aux libertés de 1978, laquelle sera modifiée par la loi du 6 aout 2004[98], permettant l'harmonisation de la réglementation informatique en Europe, rendue possible par l'adoption, sur le territoire national, de la directive européenne 95/46/CE[99] du 24 octobre 1995.

Ainsi, par une telle manœuvre, puisqu'il est possible d'apprécier le fait que « *La loi française inspira fortement le législateur européen qui a repris de nombreux principes déjà inscrits dans la loi Informatique et Libertés* »[100], il est également possible d'affirmer, avec chauvinisme et fierté, que l'actuel règlement, relatif à la protection des données personnelles, prend racine sur notre territoire national.

Le champ d'application territorial du règlement européen est fixé au sein de l'article 3 qui prévoit que « *1. Le présent règlement 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****. 2. Le présent règlement s'applique au traitement des données à caractère personnel* ***relatives 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 : a) à l'offre de biens ou de*

[98] Loi n°2004-801 du 6 aout 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.

[99] 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.

[100] N. Rispoli, *L'audit de la protection des données personnelles à l'aune du Règlement Général sur la Protection des Données*, Mémoire de Msc 2 en Audit et gouvernance des organisations, Sous la direction de Monsieur Jacques Vera, Année universitaire 2016-2017, p. 13.

services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sin de l'Union. 3. Le présent règlement s'applique 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* »[101].

Par ces dispositions, il est notable de relever que le lieu de traitement des données personnelles ne semble plus avoir d'incidence. En effet, la volonté du règlement est d'avoir un rayonnement et une portée planétaire. Bien entendu, ce dernier s'attache à protéger la « région européenne », mais pas seulement. Il ne vise pas seulement les entreprises ou établissements basés sur son territoire. Il se veut aussi méfiant, à l'échelle internationale, envers tous ceux qui souhaitent viser et cibler le marché européen. Pour le dire autrement, il ne sera désormais plus possible pour une entité d'échapper à cette législation, simplement en hébergeant un système d'information loin des frontières européennes.

9. Tout ceci conduit naturellement à s'interroger sur ce qui se passe dans les pays voisins, hors frontières nationales. En effet, il parait nécessaire, pour que l'analyse introductive du sujet soit complète, de se poser la question s'il existe d'autres régimes de droits, relatifs à cette matière, dans d'autre pays ?

Aux États-Unis, par exemple, l'impact du Règlement général sur la protection des données personnelles se fait déjà ressentir. Alors que certains sénateurs discutaient de la possibilité d'un tel règlement à l'américaine, plusieurs géants du numérique outre-Atlantique, tel que Apple, Microsoft, IBM ou encore Cisco réclament la mise en place d'un tel dispositif.
Pour exemple, le responsable juridique la dernière entreprise citée déclarait lors d'une interview que *« le RGPD a bien fonctionné, à quelques différences près,*

[101] RGPD art. 3, *préc.*

c'est aussi ce qu'il faudrait introduire aux États-Unis »[102]. Ces propos font échos à ceux, également, tenus par le directeur général d'Apple, qui lors d'une tribune s'adressait aux américains en leur avouant « *Vous méritez le respect de la vie privée en ligne* »[103]. La volonté est donc manifeste, les grandes sociétés, dont l'activité est en lien avec le numérique, conviaient hâtivement le Congrès américain d'adopter une loi fédérale sur la protection de la vie privée.

En se servant du modèle français et européen, il semble que les États-Unis prennent conscience et fassent de la confidentialité des données une priorité d'un futur, qui se doit d'être proche. Pour autant, il est de mise de ne pas s'enthousiasmer trop rapidement, puisque si l'administration Trump s'activait en ce sens, le texte américain devrait malheureusement être beaucoup moins strict que celui déjà vigueur en Europe. Pour preuve, l'ancien secrétaire américain au commerce, énonçait quelques réticences envers le Règlement européen, estimant que la mise en place d'un tel texte outre-Atlantique conduirait à « *perturber la coopération transatlantique sur la régulation financière, la recherche médicale, la coordination de services d'urgence et le commerce* »[104].

Si les États-Unis prétendent qu'un texte dont l'objectif est de protéger les données personnelles serait un frein pour le commerce, l'avis est tout autre en Europe, bien heureusement.

Le continent européen met en place un système extrêmement protecteur, en particulier au regard de la protection de la personne telle qu'elle est fixée par le champ de la Convention européenne de sauvegarde des droits de l'homme et du lien évident que la donnée personnelle entretient avec le respect de la protection de la dignité de la personne humaine. En effet, le concept de dignité, s'il s'entend naturellement au plan de la protection physique de la personne, porte en lui les éléments tout aussi fondamentaux d'une protection morale, dont l'honneur ou la

---

[102] URL : https://www.lemondeinformatique.fr/actualites/lire-apple-cisco-et-microsoft-reclament-un-rgpd-a-l-americaine-74214.html

[103] URL : http://time.com/collection/davos-2019/5502591/tim-cook-data-privacy/

[104] URL : https://www.ft.com/content/0f76f05e-d165-11e8-9a3c-5d5eac8f1ab4

vie privée ne sont finalement que des avatars[105], et qui se confrontent, naturellement avec la notion de « donnée personnelle ». La jurisprudence, a d'ailleurs eu l'occasion, au visa de l'article 16 du Code civil, de préciser ce point en consacrant que « *La sauvegarde de la dignité de la personne humaine contre toute forme d'asservissement et de dégradation est un principe à valeur constitutionnelle* »[106].

Le caractère éminemment fondamental tend donc à suggérer que la protection par le biais de la dignité se doit d'être aussi large que possible. C'est pourquoi il a très vite été question de le faire porter sur tout ce qui relève de la protection extrapatrimoniale de la personne, à commencer par ce qui relève de son intimité ou de son image[107], le principe sera par la suite étendu aux « données personnelles ».

En effet, un arrêt de la Cour européenne des droits de l'homme en date du 10 octobre 2006 précise, qu'il y a « *Violation de l'art. 8 Conv. EDH, compte tenu du rôle fondamental de la protection des données personnelles, en cas de reproduction par le juge, dans les motifs de la décision, d'extraits d'une pièce médicale confidentielle* »[108].

10. La donnée personnelle n'est donc pas une chose commune, n'est pas une chose classique au sens des dispositions du droit civil français et par conséquent doit

---

[105] « *La considération de la dignité de la personne humaine, si importante en termes de droit naturel, a pénétré de manière croissante dans le droit positif (art. 16, C. civ.)* », F. Terré, D. Fenouillet, *Droit civil : La famille*, Dalloz, 8eme édition, précis, p. 17.
« *Quant à Internet avec, dans son sillage, la circulation tourbillonnante de données personnelles détachées de leur titulaire, sans parler des profils et autres avatars, doubles des personnes réelles, ils achèvent de semer la confusion dans le repérage de ce qui fait l'identité de la personne et ce qu'on peut lui imputer en termes de droits et d'obligations* », F. Bellivier, *Droit des personnes*, Domat, Lextenso éditions, p. 19.

[106] Cons. const., 27 juillet 1994, n° 94-343/344-DC : D. 1995. 237, note Mathieu ; D. 1995. Somm. 299, obs. Favoreu.

[107] V. Civ. 1re, 20 déc. 2000, n° 98-13.875 P: *D. 2001. 885; ibid. 872, étude Gridel; ibid. Somm. 1990, obs. A. Lepage; JCP 2001. II. 10488, concl. Sainte-Rose, note Ravanas; LPA 7 mars 2001, note Derieux (5e esp.); RTD civ. 2001. 329, obs. Hauser.*

[108] CEDH., sect. II, 10 octobre 2006, L. L. c/ France, n°7508/02 : D. 2006. IR 2692 ; RTD civ. 2007. 95, obs. Hauser.

bénéficier d'un statut particulier, notamment quand elle doit être l'objet d'un contrat.

En effet, parce qu'elles représentent « *une composante d'identité et de personnalité* »[109], les données personnelles ne sont ni tangibles ni matérialisables, à cause de leur aspect. Pour autant, au même titre que les données numériques, qui désignent un format plus qu'un information[110], les données à caractère personnel peuvent être considérées comme des choses incorporelles ou immatérielles[111] et à ce titre, si tel est le cas, elles ne doivent pas être, définitivement, écartées de la sphère contractuelle.

Ainsi, la question qui se pose sera de savoir si d'abord et avant tout la donnée personnelle peut être l'objet d'un contrat, ensuite si elle peut rentrer dans le contenu d'une convention et le cas échéant il convient de s'intéresser à l'influence qu'elle va avoir sur le contrat dont elle sera l'élément.

S'il est possible de contracter sur une donnée personnelle ou que la donnée personnelle soit un élément central ou accessoire d'une convention, alors, il faudra s'interroger sur la place qu'occupera la donnée personnelle dans la convention et les contraintes que sa présence pourra générer dans le contrat.

11. C'est pourquoi il convient, dans un premier temps, de s'intéresser aux données personnelles dans la formation du contrat (Partie 1) pour ensuite faire état de l'exécution du contrat portant sur les données personnelles (Partie 2).

---

[109] J. Rochfeld, *Contre l'hypothèse de la qualification des données en tant que biens*, in A. Chaigneau et E. Netter (dir.), *Les biens numériques*, PUF, 2015, p. 221 et s.

[110] V-L. Benabou, *Entrée par effraction d'une notion juridique nouvelle et polymorphe : le contenu numérique*, Dalloz IP/IT, 2017, p. 7

[111] D. Houtcieff, *Droit des contrats*, Paradigme, 6eme édition, « manuel », p. 149.

PREMIERE PARTIE

Les données personnelles dans la formation du contrat

12. Les « données personnelles » doivent être un élément de la formation du contrat (Titre I) et donc à ce titre se plier aux exigences de droit commun dans la formation du contrat (Titre II).

TITRE 1
Les données personnelles, élément relevant du contenu du contrat

13. La donnée personnelle s'inscrit dans le contrat comme pouvant en être le « contenu » du contrat, tel que l'entend la nouvelle terminologie. Cela amène tout naturellement à imaginer que sous ce vocable, c'est tout à la fois l'objet du contrat (Chapitre 1) qui peut être concerné par la donnée, que le but du contrat que d'être en lien avec la donnée (Chapitre 2).

Chapitre 1 : La donnée personnelle en tant « qu'objet » du contrat

14. En tant qu'objet du contrat, la donnée peut être l'objet principal du contrat (Section 1), auquel cas le contrat sera particulièrement en lien avec la donnée, qu'un élément plus secondaire, la donnée étant un élément en lien avec l'objet principal du contrat (Section 2).

Section 1 : La donnée personnelle « objet » principal du contrat

15. La notion « d'objet » du contrat sera d'abord apprivoisée dans sa conception issue de la réforme de 2016 (Paragraphe 1), ce qui permettra ensuite de développer la notion de « donnée personnelle » en tant « qu'objet » principal du contrat (Paragraphe 2).

§1 : « L'objet » du contrat tel qu'il est entendu en tant que contenu contractuel issu de la réforme de 2016

16. L'article 1126 (ancien) du Code civil qui disposait que « *Tout contrat a pour objet une chose qu'une partie s'oblige à donner, ou qu'une partie s'oblige à faire ou à ne pas faire* »[112], est désormais remplacé par la formulation de l'article 1128 (nouveau) du Code civil, qui énonce que « *sont nécessaires à la validité d'un contrat : le consentement des parties, leur capacité de contracter et un contenu licite et certain* »[113].

Cette nouvelle tournure permet, immédiatement, une remarque : désormais, le Code civil ne fait plus mention directe de la notion d'objet[114]. En effet, cette évolution représente pour certains auteurs « l'innovation majeure »[115] de l'Ordonnance portant réforme du droit des contrats, du régime général et de la preuve des obligations.

Il n'est pas, simplement, question d'un changement terminologique de l'article précité, puisque, outre la disparition de la notion d'objet, figure également

---

[112] C. civ., anc. art. 1126 *(Abrogé par Ord. n° 2016-131 du 10 févr. 2016, à compter du 1er oct. 2016)*.

[113] C. civ., art. 1128, *préc.*

[114] « *Que l'article 1128 troque l'objet et la cause au profit du contenu du contrat, cela ne passe pas inaperçu* », N. Dissaux, *Contrat : formation – Détermination des conditions, Op. cit.*

[115] B. Mercadal, *Réforme du droit des contrats : Ordonnance du 10 février 2016*, Dossier pratique, 2016, Éditions Francis Lefebvre, p. 91.

l'abandon de la référence à la cause, toutes deux, au profit de ce nouveau critère qui est celui de « contenu »[116].

Aussi, comme c'est le cas pour la disparition de la cause, qui ne figure plus au sein des textes régissant le droit des contrats, celle de l'objet est aussi à déplorer[117]. Pour autant, il convient d'atténuer les propos précédents, car, si la notion « d'objet » du contrat n'est certes plus, ni insérée, ni mentionnée, dans le Code civil, elle reste, cependant, fort logiquement, toujours bien présente. En effet, ce dernier fait encore référence à ce concept, puisque, pour preuve, la conformité à un objet déterminé ou déterminable reste une condition essentielle de validité requise pour la formation d'un contrat[118]. De plus, la notion d'objet se retrouve, pour l'essentiel, dans celle de contenu, même si, et cela est regrettable, l'article 1128 du Code civil, lui-même, ne donne aucune précision concrète sur la notion[119].

17. Une lecture attentive de l'article 1128 *in fine* du Code civil conduit à se rendre compte que le législateur subordonne, désormais, la validité du contrat à l'existence d'un « *contenu licite et certain* »[120].

Si cette nouveauté qui, selon Philippe Simler « crève les yeux »[121], intéresse particulièrement l'étude de ce paragraphe relatif à l'objet du contrat tel qu'il est entendu en tant que contenu contractuel issu de la réforme de 2016, s'articule autour de la nouvelle notion de « *contenu licite et certain* », il ne faut pas pour autant négliger l'apport de la réforme du droit des obligations qui maintient, au

---

116 « *Outre les conditions de consentement et de capacité, le nouvel article 1128 issu de l'ordonnance n° 2016-131 du 10 février 2016 exige désormais un contenu licite et certain. La réforme du droit des contrats supprime la référence à la cause qui se retrouve absorbée dans les exigences relatives au contenu, à la faveur d'un glissement sémantique de l'objet vers le contenu du contrat* », G. Deharo, *Contrat judiciaire*, Répertoire de procédure civile, Septembre 2017 (actualisation : Décembre 2019).

117 V. par ex R. Cabrillac, *Droit des obligations*, Dalloz, 12eme édition, « cours », p. 51.

118 C. civ., art. 1163, *préc.*

119 B. Mercadal, *Réforme du droit des contrats : Ordonnance du 10 février 2016*, *Op cit*, p. 91.

120 S. Pellet, *Le ''contenu licite et certain du contrat''*, in *Dossier*, « *Le nouveau droit des obligations* », Droit et patr., 2016, n°258.
D. Houtcieff, *Droit des contrats*, Paradigme, 4eme édition, « manuel », p. 263.

121 P. Simler, *Commentaire de la réforme du droit des contrats et des obligations*, LexisNexis, p. 18.

sein de l'article 1128 du Code civil, la validité du contrat au concept du « consentement », mais aussi à celui de la « capacité de contracter des parties ». Une telle confirmation permet de légitimer et d'asseoir, encore un peu plus, la place accordée aux parties dans la formation d'un contrat. L'article 1128 du Code civil érige, en premier lieu, et c'est comme cela qu'il est rédigé, l'importance accordée aux parties. Un contrat ne sera pas valable si le consentement des créateurs de celui-ci fait défaut. La volonté commune d'individus qui souhaitent s'unir, en vue de la création de conventions quelles qu'elles soient, est primordiale et il faut la respecter. De plus, la vérification de l'aptitude à consentir de chacune des parties est également un élément non négligeable permettant, une fois encore, de protéger et satisfaire les intérêts des cocontractants. Ces deux notions représentent, à elles seules, ce que certains auteurs présentent de manière générale comme « la volonté des parties », c'est-à-dire que pour être parfait, le contrat doit toujours être, quoi qu'il arrive, « *voulu par les parties qui doivent y consentir* »[122].

Ainsi, dès la lecture des deux principales composantes de l'article 1128 du Code civil, il est possible d'affirmer que ce texte utilise la volonté et la capacité des individus afin de protéger ces derniers. Si la validité d'un contrat est, en priorité, soumise à de telles exigences, c'est bien parce que l'individu est l'élément-clef de la naissance d'un contrat.

18. L'Ordonnance du 10 février 2016 fait donc émerger une notion nouvelle, celle du contenu. Par-là, le législateur entend désormais regrouper, sous une même notion, les différents concepts d'objet et de cause qui étaient traités distinctement[123]. En effet, avant que ladite réforme n'intervienne, la notion de contenu permettait de regrouper les exigences légales relatives à deux conditions de validité, l'objet et la cause. Déterminer l'objet de l'engagement, c'est se demander ce que l'on veut

[122] L. Andreu et N. Thomassin, *Cours de droit des obligations*, Amphi LMD, Éditions Gualino, 4e édition 2019-2020, p. 129.

[123] « *Si les deux notions tenaient à être confondues dans le Code civil, on peut regretter que la réforme du droit des contrats n'ait pas été l'occasion de lever cette confusion en consacrant l'objet du contrat comme une notion autonome* », C. Brenner et S. Lequette, *Acte juridique – Théorie général de l'acte juridique*, Répertoire de droit civil, Février 2009.

(*quid debetur*[124]). En déterminer la cause, c'est se demander pourquoi on le veut (*cur debetur*). Désormais, le contenu constitue, à lui seul, une condition de validité.

L'ambition d'une telle innovation (et c'est également le cas pour l'ensemble de la réforme du droit des obligations de 2016) était de permettre une clarification et une simplification du droit français. Cet objectif semble, de nos jours atteint, comme le soulignent certains auteurs en énonçant à ce propos « *une fois rénové (le droit français) est incontestablement redevenu plus clair, lisible, accessible* »[125].

Pour apprécier et critiquer le résultat de l'innovation consistant à retenir la notion de contenu comme seule condition de validité du contrat, ces auteurs l'ont confronté au principe général de sécurité juridique, principe lui-même défini comme un « *idéal vers lequel le droit doit tendre en édictant des règles cohérentes, relativement stables et accessibles pour permettre aux individus d'établir des prévisions* »[126]. A ce sujet, il a pu être remarqué et analysé que la sécurité juridique se confond systématiquement avec les thématiques de l'accessibilité du droit ou encore celle de simplification[127]. Sur ces points, il est certain que les conditions relatives au principe de sécurité juridique sont remplies, la notion de contenu permettant à elle seule d'exprimer et de remplacer celles d'objet et de cause.

19. De plus, si anciennement les notions d'objet et de cause répondaient à des fonctions différentes, mais semblables, dorénavant la fusion de ces deux termes voisins, dans la seule notion de « contenu » du contrat a permis de mettre fin à certaines ambiguïtés juridiques. D'un côté, il est possible d'affilier à la notion d'objet une certaine fonction qualificative de l'obligation qui va naitre du contrat.

---

[124] « *L'objet de l'obligation est ce sur quoi elle porte. Selon la formule classique, l'objet de l'obligation répond à la question « quid debetur ? », qu'est-ce qui est dû ?* », D. Houtcieff, *Droit des contrats*, Paradigme, 5eme édition, « manuel », p. 311.

[125] F. Ancel et B. Fauvarque-Cosson, *Le nouveau droit des contrats, Guide bilingue à l'usage des praticiens*, Collection LGDJ, Edition Lextenso, p. 97.

[126] Dictionnaire du vocabulaire juridique 2020, LexisNexis, 11e édition, sous la direction de R. Cabrillac, p. 485.

[127] V. sur ce sujet, J-M. Sauvé, *La simplification du droit et de l'action administrative*, Colloque organisé par le Conseil d'État et la Cour des comptes, 16 déc. 2016, reproduit sur le site du Conseil d'État.

Pour le dire autrement, l'objet permet de répondre à la question de savoir sur quoi repose le contrat. De l'autre, plus qu'une simple volonté des parties, la cause, développée par les juristes Domat et Pothier, représente le motif ou la raison qui pousse les parties à contracter ensemble sur l'objet défini par elles. Les deux concepts, qui ne sont pas si éloignés, ont à la base une motivation similaire, mais ce rapprochement n'est pas si aisé.

Pour les anti-causalistes, dont faisait partie le juriste Planiol, l'inutilité de la notion de cause n'est plus à prouver, la cause étant confondue avec l'objet du contrat[128]. Cette partie de la doctrine démontre que le contrat se forme, seulement, à travers la réunion du consentement des parties, d'un objet et de la capacité de ces dernières. La finalité est qu'il n'y a pas de place pour la cause qui n'est pas une condition de validité du contrat.

Voilà pourquoi, marquée par l'incertitude, l'imprécision et surtout la proximité entourant ces deux notions[129], la réforme du droit des obligations n'a pas résisté à rapprocher la notion d'objet et de cause dans un seul et même concept, celui de « contenu ».

Le scepticisme énoncé précédemment, sur la notion d'objet et surtout de cause, causé par le caractère, pour le moins, obsolète, de celles-ci, est en discordance avec l'avènement de la réforme du droit des obligations[130]. Le paradoxe est simple, il existe une incompatibilité avec le projet de l'Ordonnance n° 2016-131 du 10 février et la vétusté de certains principes juridiques. Puisque le désir et l'aboutissement de l'Ordonnance concernent l'amélioration, l'harmonisation et la simplification du droit, il est normal que les notions désuètes ne participent et ne survivent pas à ce changement.

---

[128] M. Planiol, *La cause du contrat, Traité élémentaire de droit civil*, 11e éd., LGDJ, 1931, p. 396-397.

[129] « *L'obscurité de cette notion, la diversité de ses définitions selon la fonction qu'elle est amenée à remplir, en font la providence des plaideurs, parfois des juges et même des auteurs en panne d'arguments juridiques* », J. Ghestin, *Cause de l'engagement et validité du contrat*, LGDJ, 1e éd., 2006.

[130] « *Le maintien de cette expression française, contre vents et marées, semble contredire l'un des principaux dessins poursuivis par l'avant-projet, à savoir que le nouveau code redevienne un modèle exportable hors de nos frontières, qu'il constitue une source d'inspiration pour les législateurs étrangers et surtout pour le législateur européen* », B. Fauvarque-Cosson, *La réforme du droit français des contrats*, *préc*, note 21.

Pour certains auteurs, en revanche, plutôt que de renommer la cause ou de la faire implicitement disparaitre, ces derniers proposent qu'« *il serait certainement plus utile de la conserver en l'exposant au grand jour* »[131]. S'ils reconnaissent que la notion n'est pas des plus faciles à appréhender, ils indiquent toutefois qu'elle tient une véritable position, au sein du droit, à tel point qu'ils affirment que la cause est utilisée massivement chaque année par la Cour de cassation pour juger par exemple de la validité de contrats[132].

En définitive, si l'Ordonnance portant réforme du droit des obligations de 2016 écarte, au sein du nouvel article 1128 du Code civil, les concepts d'objet et de cause, au profit de celui de contenu, il semble que cette suppression ne soit pas si catégorique et que leur « esprit »[133] soit ainsi toujours présent.

20. C'est dans ce contexte qu'il peut paraitre nécessaire de conserver le terme en question, « l'objet » du contrat se retrouvant aujourd'hui au sein d'une sous-section du Code civil, intitulée « Le contenu du contrat », section qui s'ouvre par l'article 1162 qui s'intéresse à la licéité du contenu du contrat en précisant la chose suivante : « *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* »[134].

La finalité de cet article est d'interdire que les stipulations du contrat dérogent à l'ordre public, où se retrouve notamment la nécessité d'un objet licite. Si l'ambition poursuivie par ce texte parait tout à fait légitime, elle oublie néanmoins, comme le déplorent si bien Philippe Malaurie, Laurent Aynès et Philippe Stoffel-Munck par cette pensée, que « *bien que l'on dise aujourd'hui souvent le contraire, aucune société ne peut survivre sans tabous* »[135].

En traitant du « but » du contrat au sein d'une partie du Code civil, réservée au « contenu » du contrat, le législateur s'en rapporte, en réalité, à la notion de cause. Selon Christian Larroumet, « *la cause subsiste dans le mot « but », puisque la*

---

[131] URL : https://halshs.archives-ouvertes.fr/halshs-01201761/document

[132] Cass. com., 13 février 2007, n° 05-17407 ; Cass. civ., 1re, 30 octobre 2008, n°07-17.646 ; Cass. civ., 2e, 2 février 2017, n° 16-10.165 ; Cass. com., 9 octobre 2019, n° 18-14.861 ; Cass. civ., 1re, 17 février 2021, n°19-22.234.

[133] URL : https://actu.dalloz-etudiant.fr/a-la-une/article/suppression-de-la-cause-reforme-du-droit-des-contrats-du-regime-general-et-de-la-preuve-des-obligations

[134] C. civ., art. 1162, *préc.*

[135] P. Malaurie, L. Aynès et P. Stoffel-Munck, *Droit des obligations*, LGDJ, Lextenso éditions, 10e édition, p. 345.

cause du contrat, c'est-à-dire le motif principal et déterminant de la conclusion d'un contrat et, par conséquent, le but de l'opération contractuelle, peut ne pas être conforme à l'ordre public, même si les stipulations le sont »[136].

21. Réglementé aux articles 1163 à 1167 du Code civil, « l'objet » désigne, dans ces nouveaux textes, la prestation que l'une des parties s'engage à accomplir au profit de l'autre, ce qui n'est rien d'autre, finalement, que son ancienne définition. L'objet est une notion qui renferme deux aspects, à savoir, d'un côté l'objet du contrat et de l'autre l'objet de l'obligation. Voici un aperçu de ce que représentent ces deux notions. L'objet de l'obligation est entendu comme la prestation qu'une partie s'est engagée à accomplir, tandis que l'objet de l'opération contractuelle (aussi qualifié d'objet du contrat) désigne l'opération contractuelle que les parties ont réalisée, opération qu'il faut alors prendre dans son ensemble et non plus dans l'un ou l'autre de ses éléments constitutifs.

S'il est aisé de comprendre que pour exister, l'obligation doit avoir « *pour objet une prestation présente ou future* »[137], sinon quoi, « *la chose qui fait la matière du contrat n'existe pas, le contrat est nul : par exemple l'animal vendu est mort quelques instants plus tôt* »[138], l'article 1163 alinéa 2nd du Code civil impose que la prestation objet de l'obligation soit possible, déterminée ou déterminable.
L'exigence de détermination de l'objet se comprend, en effet, à défaut d'un objet déterminé, le débiteur ne saurait pas ce à quoi il s'engage et le créancier ne saurait pas davantage ce qu'il peut exiger. De la même manière, l'objet doit être possible, ainsi il ne faut pas qu'il existe une impossibilité de faire ou de ne pas faire ce qu'on s'est engagé à faire ou à ne pas faire.
Il est à noter, dans le fil conducteur du développement précédent, qu'à travers le dernier alinéa de l'article susvisé, le Code civil offre une certaine souplesse. C'est

---

[136] C. Larroumet, S. Bros, *Traité de droit civil, Les obligations, Le contrat*, Economica, 9eme édition, « corpusdroitprivé », p. 411.

[137] C. civ., art. 1163 al. 1er, *préc.*

[138] A. Bénabent, *Droit des obligations*, précis Domat, LGDJ, Lextenso éditions, 18e édition, p. 140.

ainsi qu'est considéré comme certain l'objet qui est déterminable au jour de l'exécution sans que celui-ci soit, pour autant, immédiatement déterminé[139].

Les articles 1164 et 1165 traitent de la détermination du prix. Si le nouveau Code civil consacre plusieurs dispositions à la détermination du prix, il n'admet finalement la disposition d'une fixation unilatérale que de manière très limitée.
D'une part, l'article 1164 alinéa 1er nouveau dispose que « *Dans les contrats cadre, il peut être convenu que le prix de la prestation sera fixé unilatéralement par l'une des parties, à charge pour elle d'en motiver le montant en cas de contestation* »[140]. Il convient de noter tout d'abord que cette disposition ne concerne que les contrats cadre.
Ensuite le texte prévoit que la partie qui fixe unilatéralement le prix doit pouvoir en motiver le montant, en cas de contestation ; cette obligation de motivation opérant ainsi un renversement de la charge de la preuve (ce n'est plus à celui qui se plaint du prix fixé de démontrer qu'il est abusif, mais à l'autre partie de le justifier).
Enfin l'ordonnance vient préciser la sanction en cas d'abus dans la fixation du prix.

D'autre part, l'article 1165 nouveau prévoit, s'agissant des contrats de prestation de service qu'à défaut d'accord entre les parties avant leur exécution, le prix peut être fixé par le créancier, à charge pour celui-ci d'en motiver le montant. Cette disposition repose sur l'idée qu'il est souvent difficile, dans les contrats de prestation de service, et en particulier, dans les contrats d'entreprise, de déterminer à l'avance l'étendue des diligences à accomplir. Aussi, faut-il laisser au prestataire la possibilité de déterminer le prix à l'issue de sa prestation.

22. Les articles 1166 et 1667, enfin, ont trait à la qualité de la prestation et à l'indexation du prix du contrat. Dans sa nouvelle version, le Code civil précise

---

[139] V. en ce sens, Cass. 1er civ., 16 juillet 1964, *Bull. civ.,* I, n°322 (au sujet d'objets vendu non décrits et entreposés dans un garde meuble) ou Cass. 3e civ., 15 février 1984, *Bull. civ.,*III, n°41 (au sujet de la vente d'une superficie de terrain à délimiter sur une parcelle).

[140] C. civ., art. 1164 al. 1er *(Ord. no 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

désormais les critères pour déterminer la qualité de la prestation à l'article 1166 nouveau, sans se référer à l'idée d'une qualité moyenne.

Cette disposition prévoit en effet que lorsque la qualité de la prestation n'est pas déterminée ou déterminable en vertu du contrat, le débiteur doit offrir une prestation conforme aux attentes légitimes des parties en considération de sa nature, des usages et du montant de la contrepartie. Ces critères induisent donc que la qualité attendue de la prestation ne saurait être la même pour tous les contrats. Il n'est en effet pas possible d'attendre la même qualité de prestation selon le prix payé.

Concernant la question de l'indexation du prix du contrat, la réforme, par l'article 1167 du Code civil, précise que lorsque le prix ou tout autre élément du contrat doit être déterminé par référence à un indice qui n'existe pas ou a cessé d'exister ou d'être accessible, celui-ci est remplacé par l'indice qui s'en rapproche le plus, ce qui n'est qu'une consécration de la jurisprudence antérieure en la matière[141].

23. S'il est possible de constater que le terme a, quasiment définitivement, disparu du Code civil, pour le moins, en ce qu'il n'est plus une condition de validité du contrat, « l'objet » de l'obligation en tant que contenu contractuel reste finalement une constante.

A ce sujet en effet, certains auteurs apportent, autour de la suppression de la notion d'objet, un regard assez tranché et quasi-critique en affirmant que « *son abandon à l'occasion de la réforme ne suscite que peu de regrets, la notion de « contenu du contrat », voire tout simplement de contrat, étant parfaitement à même de remplir les fonctions fantomatiques autrefois dévolues à l'objet du contrat* »[142].

Touché par l'Ordonnance portant réforme du droit des obligations, si l'objet du contrat, a été contraint de s'effacer, notamment du Code civil, il n'a pas, pour autant, définitivement disparu. C'est en effet par l'émergence d'une nouvelle

[141] Cass. civ. 1ere, 9 novembre 1981, n°80-11.060 : *Bull. civ. I, n°332 ; RTD civ. 1982. 601, obs. Chabas* ; Cass. civ. 3e, 22 juillet 1987, n°84-10.548 : *Bull. civ. III, n°151*.

[142] D. Houtcieff, *Droit des contrats*, *Op cit*, p. 311.

notion, à savoir celle de contenu du contrat, que l'abandon au concept d'objet du contrat, comme référence, est compensé.

Si l'approche relative à la notion d'objet du contrat a changé depuis cette nouvelle conception issue de la réforme de 2016, il n'en reste pas moins qu'elle reste actuelle et dans l'ère du temps. Voilà pourquoi, il convient, désormais, de se demander s'il est possible pour une donnée personnelle de se muer en tant qu'objet principal du contrat.

§2 La donnée personnelle en tant « qu'objet » principal du contrat

24. Afin d'étudier et d'apprécier concrètement la donnée personnelle en tant « qu'objet » principal du contrat, il convient de faire un retour en arrière sur l'article 4 du Règlement général sur la protection des données[143]. Si une donnée personnelle se définit comme « *toute information se rapportant à une personne physique identifiée ou identifiable* »[144], est-ce pour autant une chose qui pourrait s'entendre comme un « objet » principal du contrat ?

25. Le Règlement UE 2016/679 s'efforce de clarifier ce qu'est une « *personne physique identifiable* » et ajoute, pour ce faire, que celle-ci sera celle « *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* »[145].

Il est donc évident que par l'article présenté, le règlement cité, entreprend une intention de clarté. Si la notion de « donnée personnelle » semble vague dans le langage commun, le Règlement européen, toujours dans un souci de protection, l'explique avec transparence.

En effet, aux vues des multiples manifestations qu'il en fait, le règlement laisse, volontairement, à penser que la notion de « donnée personnelle » doit s'entendre et se comprendre de façon très large.

26. Attention toutefois, il convient, pour éviter l'émergence d'une quelconque confusion sur la notion de « donnée personnelle », de s'intéresser à une remarque pertinente qui fait état de l'ampleur et de l'étendue de ladite notion, illustrant, par ailleurs, l'esprit dudit règlement. Il s'agit de ne pas commettre « l'erreur courante », consistant à penser de façon maladroite que « *les données*

[143] RGPD art. 4, *préc.*

[144] *Ibid.*

[145] *Ibid.*

personnelles sont celles qui identifient une personne » alors « *qu'il s'agit en fait des données relatives à une personne* »[146].

Si la distinction, entre les données qui identifient une personne et celles qui sont relatives à une personne, peut sembler infime et sans incidence, elle revêt pourtant une importance, qui, si elle est mal comprise, fausse toute la perception au sujet des données personnelles.

Bien entendu, l'identification d'une personne se fera, grâce à des éléments qui lui correspondront, c'est-à-dire des données qui lui seront, par essence, propres. Il n'est en effet possible d'identifier un individu par rapport à un autre que lorsque toutes les informations de ces derniers sont connues, permettant ainsi de les départager (c'est le cas par exemple pour des personnes homonymes qui auront le même nom, le même prénom, parfois la même nationalité, mais n'auront nécessairement pas le numéro de sécurité sociale, ni la même adresse, etc.).

Cependant, et c'est là que la distinction est importante, il est possible d'identifier une personne sans pour autant en connaitre l'ensemble de ses données personnelles. Une simple expérience permet de se rendre compte des propos évoqués.
Il est en effet possible de déterminer, au sein d'un groupe, des individus et de séparer ces derniers en plusieurs catégories en fonction par exemple de leurs sexes, masculins et féminins, ou de leurs âges, majeurs et mineurs, sans pour autant être intrusif pour leurs données personnelles. Toutefois, pour chaque individu, le sexe ou l'âge fait partie intégrante de la personne et représente une information propre à chacun et peut, en ce sens, représenter une donnée personnelle. Ce type de procédé démontre qu'il est possible d'atteindre les données personnelles des individus sans les accaparer, mais aussi et surtout qu'il est possible de distinguer un individu par rapport à un autre à travers quelques informations qui le caractérisent, sans pour autant les connaitre toutes.

[146] F. Mattatia, *RGPD et droit des données personnelles*, *Op cit*, p. 54.

27. La confusion entre les données qui identifient une personne et celles relatives à une personne étant illustrées, il parait opportun d'évacuer une autre caractéristique qui ne rentre pas dans le champ de la définition des données personnelles. En effet, si la notion de donnée personnelle doit s'entendre et se comprendre de façon très large, il convient pour autant d'exclure, dès à présent, de sa définition et donc de retirer définitivement du champ d'application de l'article 4 du Règlement européen, les données strictement anonymes, c'est-à-dire celles qui ne peuvent pas être réidentifiées et cela de manière irréversible[147].

A ce sujet d'ailleurs, pour expliquer la vision modernisée du fameux règlement, c'est-à-dire moins restreinte que l'était sur ce point la directive de 1995[148], la pensée suivante considère qu'« *une donnée, même rendue anonyme, conserve ainsi son caractère personnel si l'anonymat est réversible et peut être éventuellement levé, non seulement par le responsable du traitement, ce qui est évident mais aussi par une autorité disposant de pouvoirs d'enquête et de croisement avec d'autres fichiers, ou disposant d'une puissance technologique permettant d'espionner ou de percer le chiffrement du traitement considéré [149]*».

28. Ainsi, pour reprendre cette analyse, une personne peut-elle être identifiée directement, grâce à l'utilisation de son état civil (son nom, prénom, sexe, âge, ou encore sa nationalité) ou indirectement, par l'emploi d'un surnom, un mot de passe, un identifiant, un numéro (quel qu'il soit), une adresse de domicile, une adresse IP, une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique (sa taille, sa couleur de cheveux), psychologique, génétique, psychique, économique, culturelle et sociale, ou encore par la voix ou l'image.

Plus encore, l'identification d'une personne physique peut être réalisée à partir d'une seule donnée, c'est le cas pour un numéro de sécurité sociale ou pour l'ADN

---

147 N. Martial-Braz et J. Rochfeld, *Droit des données personnelles : les spécificités du droit français au regard du RGPD*, Collection Dalloz Décryptage, Edition Dalloz, p. 32.

148 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, *préc.*
Cette directive de l'Union européenne (abrogée le 25 mai 2018) constituait le texte de référence en matière de protection des données à caractère personnel.

149 F. Mattatia, *Traitement des données personnelles : le guide juridique*, Éditions Eyrolles, p.31.

(situation où l'ADN permet de trouver des identifications en matière civile telle que la preuve de paternité ou en matière pénale, pour la découverte de criminel[150]), mais aussi, à partir du croisement d'un ensemble de données, ce qui est le cas quand une personne réside à l'adresse présupposée, que cette personne est née tel jour, qu'elle est abonnée à tel magasine ou qu'elle milite au sein de telle association.

29. La notion de donnée personnelle peut, également, s'appliquer indirectement à une personne, c'est par exemple le cas concernant l'ensemble des données qu'il convient d'identifier comme étant des données « déduites »[151]. Ces données déduites regroupent notamment des avis, des appréciations, des évaluations ou des commentaires, qu'il faut assimiler pour la plupart aux forums ou aux blogs et qui si elles ne s'adressent pas directement à une personne, si elles ne se rattachent pas intrinsèquement à une personne, sont des données qui s'en rapportent. Si les données déduites ne sont donc, en apparence, pas des données personnelles, il est fondamental de les définir comme telles à partir du moment où elles traitent d'informations relatives aux individus.

30. Toutes les informations présentées, en amont, reflètent la vie privée d'une personne, c'est-à-dire ses données personnelles. Puisque toutes les caractéristiques touchant, visant une personne ou émanent de celle-ci rentre dans cette catégorie, il est compréhensible que le règlement général sur la protection des données personnelles en dresse une liste limitative, mais, toutefois, non exhaustive. Cette largesse, bienvenue, a cependant un effet inconvenant facilitant la critique, à savoir que sur ce dernier point, le règlement semble flou ou, pour le dire avec moins de virulence, timide.

Il faut comprendre que ce ressenti est normal puisque ledit règlement vise à protéger toutes les informations relatives aux personnes et ce sans en oublier

---

[150] Pour rappel toutefois, aux termes des dispositions de l'article 16-10 du Code civil, « *L'examen des caractéristiques génétiques d'une personne ne peut être entrepris qu'à des fins médicales ou de recherche scientifique* ». Et qu'au demeurant l'accord de la personne doit être recueilli.

[151] N. Martial-Braz et J. Rochfeld, *Droit des données personnelles : les spécificités du droit français au regard du RGPD*, *Op cit*, p. 32.

aucune. Aussi, il n'est pas anodin que la nature même de « donnée personnelle » soit visée dans son aspect le plus large, l'avis[152] rendu à Bruxelles par le Groupe de travail Article 29 sur la protection des données, dit G29, en témoigne et permet de se rendre compte des différentes acceptions regroupées dans la seule notion de donnée personnelle puisque ce dernier « *reconnait la nécessité de mener une analyse approfondie du concept de données à caractère personnel* », concept aux pratiques européennes comportant « *un certain degré d'incertitude et de diversité*[153] ». Une des missions principales de ce groupe de travail (G29) est donc de détailler au mieux la notion de donnée personnelle, dans un souci de bonne application et d'harmonisation des règles européennes. L'enjeu est d'éviter que ne se créée une confusion autour de la notion de donnée personnelle sur la scène européenne, ce qui pourrait nuire à sa protection, alors que c'est pourtant l'un des objectifs majeurs du Règlement général sur la protection des données.

Dans un souci d'intelligibilité et pour favoriser une meilleure compréhension de ce que recouvre, en pratique, la notion de données personnelles, une brève compilation regroupant quelques exemples et informations est proposée par un auteur spécialiste en la matière[154]. Le but de ce travail est de mettre en lumière et de retranscrire, en fait, les différentes informations dégagées et qualifiées par le G29 comme étant des données personnelles. Cette multitude d'exemples qui dévoile l'hétérogénéité de la notion de données personnelles témoigne du caractère évasif, mais non équivoque, de la définition posée par le règlement européen. En effet, si les données personnelles s'apprécient au travers de plusieurs représentations, son champ est toutefois précis et restreint.

La définition de la notion de donnée personnelle étant posée, notamment à travers la diversité qui caractérise celle-ci, il convient désormais de poursuivre l'analyse

---

[152] Groupe 29, *Avis 4/2007 sur le concept de données à caractère personnel*, WP 136, 20 juin 2021, p. 3.

[153] URL : https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp136_fr.pdf

[154] *« Sont des informations qualifiées de données à caractère personnel les enregistrements de conversations téléphoniques tels que l'enregistrement de la voix de clients ou salariés, les images de vidéosurveillance pour autant que les individus soient reconnaissables, la valeur d'un bien (une maison constituant le patrimoine d'une personne permettant de déterminer si une personne est imposable), les informations issues de techniques de segmentation comportementale, la publication de clichés radiographiques portant le prénom d'une patiente, une adresse IP permettant d'identifier l'abonné d'un fournisseur d'accès à internet, ou encore des données pseudonymisées, c'est-à-dire des données désignées par un code »,* G. Desgens-Pasanau, *La protection des données personnelles : le RGPD et la loi française du 20 juin 2018*, *Op cit*, p. 17.

en question des données personnelles en tant qu'objet principal du contrat, au prisme, cette fois ci, non pas de l'objet mais de la chose.

31. Il convient alors de s'interroger sur ce qu'est une « donnée personnelle » en tant que chose ? Afin de répondre à cette question, il est intéressant de s'arrêter un instant sur une décision rendue par la Cour de cassation.

Par un arrêt rendu le 25 juin 2013, la Chambre commerciale affirme, au sein de sa solution, que « *Tout fichier informatisé contenant des données à caractère personnel doit faire l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés (CNIL)* » et les Hauts magistrats d'ajouter « *que la vente par la société X d'un tel fichier qui n'ayant pas été déclaré, n'était pas dans le commerce, avait un objet illicite* »[155].

Cette solution, rendue au visa de l'article 1128 du Code civil, rapproche la notion de « donnée personnelle » et celle de contenu « licite et certain ». En effet, par cet arrêt, les Hauts magistrats réunissent la notion de « donnée personnelle » et celle d'extracommercialité. Si en 1804 le principe de l'extracommercialité était qu'on ne pouvait disposer de certaines choses, cette solution semble vouloir dire qu'il n'est pas possible de disposer de certaines choses n'importe comment.

Aussi, la donnée personnelle n'est donc pas une chose (ou une information) qui n'est pas « hors commerce ». Il est donc possible d'en disposer, mais à certaine condition, par exemple en faisant une « *déclaration auprès de la Commission nationale de l'informatique et des libertés (CNIIL)* ».

32. Le Règlement européen permet donc qu'une donnée personnelle soit « objet » principal du contrat, puisque rien n'interdit le contraire. La seule restriction ou obligation imposée par, tant les juridictions que le règlement, est que la « donnée personnelle » doit avoir un « objet », entendu en tant que contenu, « licite et certain »[156].

---

[155] Cass. com. 25 juin 2013, n° 12-17.037, à paraître au Bulletin, D. 2013. 1867, note G. Beaussonie ; *ibid.* 1844, point de vue P. Storrer.

[156] C. civ., art. 1128, *préc.*

Au vu de ce qui précède, s'il est possible de contracter sur une « donnée personnelle » lorsque celle-ci est entendue en tant « qu'objet » principal du contrat, il est déterminant de respecter le « leitmotiv » dudit règlement, c'est-à-dire de ne pas altérer la protection des données à caractère personnel.

33. Après avoir analysé la compatibilité entre la donnée personnelle et l'établissement d'un contrat, lorsque celle-ci en est l'élément principal, il ne faut pas oublier de souligner que d'autres règles de droit commun s'imposent pour la réussite d'une telle opération.

C'est notamment le cas pour l'un des plus grands principes du droit français énoncé, au sein de l'article 9 alinéa 1er du Code civil, en ces termes, « *Chacun a droit au respect de sa vie privée* » et dont l'irrespect entrainerait l'annulation de tous contrats. En ce sens, un contrat dont l'objet (le contenu) porterait sciemment atteinte à la vie privée serait naturellement illicite. Pour le dire autrement, un contrat qui repose sur une « donnée personnelle », en tant qu'objet, serait illicite si « la donnée personnelle » porte atteinte à la vie privée de la personne concernée. Le respect de la vie privée s'impose donc naturellement aux « données personnelles ».

34. De son coté, dans le fil conducteur de cet article, le présent règlement, toujours dans ce souci de protection met en lumière le « consentement » de la personne concernée, entendu comme « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* »[157].

Des lors, lorsqu'une personne contracte sur ses données personnelles, entendues comme « objet principal » du contrat, elle doit le savoir et le faire savoir. Sans ce consentement, le contrat ne tient pas. Qu'en est-il lorsque la donnée est un élément secondaire du contrat ?

[157] RGPD art. 4, *préc.*

Section 2 : La donnée personnelle « objet » secondaire du contrat

35. Afin de caractériser les situations dans lesquelles la donnée personnelle est « objet » secondaire du contrat, il convient de s'intéresser aux obligations dont la donnée personnelle est un accessoire (Paragraphe 1), pour ensuite en démontrer l'impact sur le droit des obligations (Paragraphe 2).

§1 Les obligations dont la donnée personnelle est un accessoire

36. S'il a été exprimé précédemment que la donnée personnelle peut faire office d'objet principal du contrat, cette affirmation est-elle vraie lorsque la donnée personnelle est entendue comme un « objet » secondaire (ou accessoire) du contrat ?

Le Règlement général sur la protection des données ne s'est pas focalisé seulement sur la protection de la « donnée personnelle » en tant quel tel, ce règlement encadre et protège aussi, fort heureusement, les contrats qui font référence à cette notion.

37. L'une des grandes logiques du Règlement UE 2016/679 réside, entre autres, dans la notion de « responsabilité »[158]. En effet, dans l'objectif d'accroitre et d'atteindre une protection sans faille des « données personnelles », ce dernier propose et impose une marche à suivre pour tous types d'obligations qui seraient en contact avec l'utilisation de données personnelles.

[158] RGPD art. 82, al. 1er, *préc.*

Si le droit commun, spécifiquement les droits civil[159] et pénal[160], font déjà l'éloge de la notion de « responsabilité » pour un chef d'entreprise, par exemple, le règlement continue cette voie en l'appliquant d'abord aux « données personnelles » puis aux responsables de traitements.

Ainsi le règlement général sur la protection des données fixe-t-il, à son tour, un cadre protecteur pour les informations aussi sensibles que peuvent l'être les « données personnelles ».

Aussi, voici une présentation des différentes obligations qui font, désormais, référence à la notion de « donnée personnelle », sans que celle-ci en soit « l'objet » principal, mais bien l'objet « secondaire ».

38. Tout d'abord, chronologiquement, la mise en place du règlement général sur la protection des données impose de constituer un « registre de traitements de données »[161].

La tenue d'un registre des activités de traitement est une nouvelle obligation imposée par l'article 30 du règlement européen qui le présente en ces mots : *« Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités du traitement effectués sous leur responsabilité »*[162]. Concrètement, si le registre soumis par celui-ci « *ne présente pas beaucoup de particularité autres que de nécessiter un énorme travail de recensement de l'ensemble des traitements mis en œuvre (et non des applications informatiques utilisées par une entreprise – même si cela donne des indications)* »[163], une particularité se dégage tout de même.

---

159 « *Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer* », C. civ., art. 1240 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

160 « *Le fait de procéder ou de faire procéder à un traitement de données à caractères personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 € d'amende* », C. pén., art. 226-17 *(L. n° 2004-801 du 6 août 2004, art. 14)*.

161 URL : https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf

162 RGPD art. 30 (1.), *préc.*

163 URL : https://www.donneespersonnelles.fr/3-registres-rgpd-devez-mettre-place

L'objectif de ce registre n'est pas, seulement ni simplement, de créer une compilation des traitements réalisés, l'objectif est aussi de façonner plusieurs catégories de traitements afin d'en faciliter la compréhension et l'usage par les organes de contrôle tel que la Commission nationale informatique et des libertés (CNIL). A ce sujet, le souhait de simplicité du Règlement européen est mentionné à travers l'idée de « *granularité du registre (qui) recouvre une « activité de traitement, et non chaque traitement isolément* »[164], ce qui résume et traduit l'envie d'avoir différentes catégories et non une multitude de traitements sans réalité de classification.

Pour la mise en place du registre des activités de traitement, il est possible (voire très conseillé) de s'armer de sous-traitants afin de coopérer et ainsi faciliter la réalisation de cette tâche. Cette possibilité est en effet affirmée, toujours, par l'article 30 dudit Règlement qui précise que « *Chaque sous-traitant et, le cas échéant, le représentant du sous-traitant tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement* »[165], cet article se prolongeant en énumérant la liste d'informations qu'il est essentiel de conserver (*considérant a) à d)*).

Au sein de l'étude des obligations dont la donnée personnelle est un accessoire, le contrat de sous-traitance apparait, chronologiquement et naturellement, comme la première obligation, sous l'emprise du Règlement protecteur des données personnelles lorsque celui-ci a pour « objet » secondaire l'utilisation de « donnée personnelle ».

39. Une analyse spécifique offre la possibilité de mettre ces idées en exergue à travers le contrat de sous-traitance. Au sens de l'article 1er de la loi n°75-1334 du 31 décembre 1975, « *la sous-traitance est l'opération par laquelle un entrepreneur confie par un sous-traité, et sous sa responsabilité, à une autre personne appelée*

[164] F. Mattatia, *RGPD et droit des données personnelles*, *Op cit*, p. 248.

[165] RGPD art. 30 (2.), *préc.*

sous-traitant l'exécution de tout ou partie du contrat d'entreprise ou d'une partie du marché public conclu avec le maitre de l'ouvrage »[166].

Le contrat de sous-traitance doit donc naturellement se soumettre au règlement général sur la protection des données puisqu'un sous-traitant est le gardien ou l'utilisateur de « données personnelles », données qui n'appartiennent ni à son client, ni à lui-même.

Le sous-traitant engage donc sa responsabilité au même titre que l'entrepreneur à qui les « données personnelles » vont être confiées, tout en sachant qu'un tel devoir s'est d'autant plus accru ces dernières années par « *l'émergence de nouveaux outils numériques, à l'instar du cloud computing*[167] », conduisant ainsi « *la Commission européenne comme les autorités de contrôles à s'interroger sur les obligations particulières des sous-traitants* »[168].

Voilà en quoi le « contrat de sous-traitance » et plus particulièrement le « contrat de sous-traitance portant sur les données personnelles » est une des obligations dont la donnée personnelle est « objet » secondaire du contrat. Marquée par les récentes évolutions techniques et par la sensibilité des données manipulées, il est fort logique qu'une telle obligation soit tributaire du règlement général sur la protection des données pour en assurer la protection.

40. Ensuite, il convient de confronter la protection des données personnelles d'un contrat particulier, qui sans y faire référence, à proprement parler, fait une utilisation permanente de la « donnée personnelle ». Cette obligation spécifique qu'il appartient désormais de détailler est le contrat de travail.

---

[166] Art. 1er, loi n°75-1334 du 31 décembre 1975 relative à la sous-traitance.

[167] Le « *cloud computing* » (en français « informatique en nuage » ou « informatique dans les nuages ») est, selon la définition officielle de la Commission générale de terminologie et de néologie, 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 » (Journal Officiel du 6 juin 2010).

[168] G. Desgens-Pasanau, *La protection des données personnelles : le RGPD et la loi française du 20 juin 2018*, *Op cit*, p. 50.

Ce dernier désigne une convention par laquelle une personne, le salarié, s'engage à travailler pour le compte et sous la direction d'une autre, l'employeur, contre rémunération[169].

41. Il se comprend que durant les différentes phases de ce contrat, du recrutement au licenciement, la protection des « données personnelles » se veut une notion essentielle. Salarié et employeur doivent assurer ensemble une relation transparente et là encore, l'utilisation de « donnée personnelle » caractérise cette convention, sans pour autant y être l'élément clef.

En effet, d'un côté, le salarié est obligé de délivrer des informations confidentielles à son égard à son employeur, ne serait-ce que ses noms, prénoms, adresse, coordonnées, numéro de sécurité sociale ou encore son relevé d'identité bancaire.
De l'autre, l'employeur délivre aux salariés des informations confidentielles concernant son entreprise ou sa société.

Plus encore, la relation de travail est une interaction de plusieurs personnes, aussi bon nombre de personnes ont accès aux « données personnelles » de chacun.

Si le contrat de travail est une obligation qui fourmille de situations dans lesquelles la donnée personnelle est « objet » secondaire du contrat, il convient de s'intéresser à une situation en particulier ayant fait l'objet d'une petite « saga » jurisprudentielle en France, à savoir le cas de la correspondance et la messagerie personnelle des salariés.

42. Consacré par l'arrêt « Nikon » du 2 octobre 2001[170], le secret des correspondances[171] est une des libertés fondamentales du salarié, en ce sens que « *le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité*

---

[169] « *Le contrat de travail est soumis aux règles du droit commun. Il peut être établi selon les formes que les parties contractantes décident d'adopter* », C. trav., art. L. 1221-1.

[170] Cass. soc., 02 octobre 2001, n°99-42.942 *: Bull 2001 V n° 291 p.233*.

[171] S. Chatry et A. Robin, *Introduction à la propriété intellectuelle,* Bruylant, 2e, Collection Paradigme, 2021, n° 373.

de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur ».

Premièrement protégé, le secret des correspondances allait voir, quelques années plus tard, son hégémonie remise en cause par l'instauration par la Haute juridiction d'une véritable présomption du caractère professionnel des courriels adressés ou reçus par le salarié sur son ordinateur permettant ainsi à l'employeur « *de les ouvrir hors la présence de l'intéressé, sauf s'ils sont identifiés comme personnels* »[172]. En effet, si le secret de cesdites correspondances était, préalablement, immunisé, notamment par la garantie et le soutien de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales[173] et l'article 9 du Code civil[174], l'avènement de la révolution numérique a causé l'effacement progressif de la portée du célèbre arrêt « Nikon ». L'utilisation intensive des moyens technologiques en entreprise transformant, faisant évoluer, le rapport de force entre d'un côté la préservation de la vie privée du salarié et de l'autre la défense de l'intérêt de l'employeur, au profit de ce dernier, par l'institution de la présomption précitée.

Mais plus récemment, peut être sous l'influence masquée du Règlement général sur la protection des données, une résurgence de la jurisprudence « Nikon » s'est établie. En effet, par arrêt du 26 janvier 2016[175], la chambre sociale de la Cour de cassation « *érige le secret des correspondances en rempart contre les intrusions de l'employeur dans la vie personnelle du salarié, quand bien même l'ingérence serait justifiée par le trouble causé à la bonne marche de l'entreprise* »[176].

---

[172] Cass. soc., 26 juin 2012, n°11-15.310 ; voir également Cass. soc., 16 mai 2013, n°12-11.866.

[173] Art. 8, Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

[174] C. civ., art. 9, *préc.*

[175] Cass. soc., 26 janvier 2016, n°14-15.360.

[176] URL : https://larevue.squirepattonboggs.com/messages-personnels-des-salaries-la-jurisprudence-nikon-n-est-pas-tout-a-fait-morte_a2857.html

L'analyse de cette jurisprudence démontre que, sur le point relatif aux secrets des correspondances, celle-ci est étonnement en phase avec l'objectif du Règlement européen. Même si le règlement ne traite pas directement de ces questions-là, il a par essence vocation à protéger les données personnelles des salariés, donc à protéger le secret de leurs correspondances et messageries. Alors que l'article 68[177] de la loi du 7 octobre 2016 pour une République numérique prône et confirme la confidentialité et le secret des correspondances électroniques privées, dans un même temps, le Règlement UE 2016/679 encadre la transmission de telles informations. En effet, si le salarié bénéficie d'un véritable droit d'accès[178], l'employeur joui, à son tour, d'un pouvoir de limitation afin d'éviter que la sollicitation du salarié en question ne porte atteinte aux droits et libertés d'autrui, au secret des affaires ou encore à la propriété intellectuelle[179]. Ainsi l'employeur pourra, à juste titre, refuser de communiquer un document qui contiendrait par exemple les données de plusieurs autres salariés. Le Règlement général sur la protection des données offre donc un droit de regard des salariés quant à leurs données personnelles mais permet également une maitrise de celles-ci par l'employeur.

43. Sur ce même sujet, une critique est toutefois envisageable à l'encontre d'une récente décision rendue par la Cour européenne des droits de l'homme (CEDH). Cette dernière a, en effet, affirmé par un arrêt du 22 février 2018 « *qu'un employeur peut consulter les fichiers d'un salarié, en son absence, s'ils ne sont pas identifiés comme étant privés* »[180]. La justification de cette décision s'entend, notamment parce qu'elle repose sur le droit d'ingérence de l'employeur, prévue par les articles, combinés, L. 1121-1[181] et L. 1321-3[182] du Code du travail, mais également par la présomption, instaurée par la jurisprudence[183], du caractère

---

177 Art. 68, Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

178 RGPD art. 15, *préc.*

179 RGPD consid. 63, *préc.*

180 CEDH, 22 février 2018, n°588/13, Libert c/ France.

181 C. trav., art. L. 1121-1.

182 C. trav., art. L. 1321-3.

183 « *Les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors sa présence* », Cass. soc., 18 oct. 2006, n°04-48.025.

professionnel des dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition, cependant en l'espèce le rejet du pourvoi formé par le requérant semble sévère. Il a été, en effet, reproché à ce dernier d'avoir nommé l'ensemble de son disque dur par l'appellation « données personnelles », ce qui, en réalité, ne conférait pas « *un caractère personnel à l'intégralité des données qu'il contient* ». La frustration est d'autant plus importante pour ce salarié puisque par cette affaire, la Cour de Strasbourg a tout de même relevé au grand jour, son identité (à savoir ses nom et prénom, sa date de naissance, son lieu de résidence, son emploi et le contenu du dossier en question) en l'absence d'anonymisation de la décision de justice, ce qui est un comble !

Si cette décision rendue par la Cour européenne des droits de l'homme semble aller à contre-courant de la jurisprudence française, notamment à l'encontre du mouvement jurisprudentiel créé par l'arrêt « Nikon », pour certains auteurs en revanche, cette décision démontre « *que le dispositif juridique français permet un équilibre entre le besoin de protection de la vie privée des salariés et l'intérêt légitime de l'employeur de s'assurer d'un usage non abusif des équipements informatiques mis à la disposition de ses salariés* »[184].

44. L'importance du Règlement général sur la protection des données se fait, une fois de plus, ressentir. Tel un véritable guide, un référent, ce dernier offre, tant aux employeurs qu'aux salariés, les démarches à suivre afin que l'un et l'autre se protègent et défendent ses intérêts. Si la politique entrepreneuriale libérale, chère aux employeurs, se comprend, elle doit être encadrée pour éviter toutes dérives, notamment éviter que les droits des salariés soient bafoués. C'est, encore, en cela, que le règlement permet aux personnes concernées de voir leurs données personnelles respectées.

Au sein d'un chapitre 3, qui sera, en partie, évoqué *a postériori* dans cette étude, le Règlement UE 2016/679 traite, d'une part « *des droits de la personne*

[184] URL : https://www.village-justice.com/articles/utilisation-ordinateur-professionnel-cedh-valide-jurisprudence-francaise,28375.html

concernée »[185], mais il met également l'accent, par une deuxième section qui s'ouvre sur l'article 13, à propos des « *informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée* »[186]. Cette exigence démontre, une fois encore, que certaines catégories de personnes, dites plus « faibles », en l'occurrence ici les salariés, bénéficient à travers le présent règlement d'une protection accrue de leurs données personnelles.

Voilà, par ces différentes explications, comment et en quoi le règlement général sur la protection des données se doit de contrôler le contrat de travail, celui-ci étant une obligation dont la « donnée personnelle » est accessoire prépondérant.

Fort heureusement, le Règlement européen n'est pas un texte fermé. La lecture qui peut et doit en être faite, offre une certaine souplesse et permet ainsi une certaine adaptabilité à toutes circonstances, notamment pour ce qui a été précédemment évoqué, aux évolutions technologiques, sociétales ou encore, de façon plus négative, aux différentes crises telle que la pandémie liée au coronavirus (Covid-19).

45. Dans un autre domaine, mais tout aussi important, la question des « données personnelles » est omniprésente, c'est pourquoi il convient, dès maintenant, de s'intéresser au droit médical. Dans le secteur de la santé, le patient est l'acteur central et toutes les informations qui lui sont relatives sont collectées puis utilisées, dans le but d'aider ce dernier.
Ainsi les dispositions de l'article L. 1110-4 du Code de la santé publique rappellent-elles ce principe en énonçant, au sein de l'alinéa 1er, que dans la relation médicale, qui de fait s'analysera comme un contrat, le patient dispose d'une protection particulière de ses données.
La protection des données de santé du patient s'effectue au prisme du droit au respect de sa vie privée, ainsi qu'au respect du secret des informations de celui-ci, « *I. – Toute personne prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou un organisme concourant à la*

[185] RGPD. Chapitre 3, Droits de la personne concernée, *préc.*
[186] RGPD art. 13, *préc.*

prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code, le service de santé des armées, un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 321-1 du code de l'action sociale et des familles a droit au respect de sa vie privée et du secret des informations le [la]concernant »[187].

Ce texte qui encadre le droit au secret médical s'applique pour l'ensemble du corps médical, c'est-à-dire qu'il s'impose à différents acteurs de la chaine médicale, pour un professionnel, un établissement ou encore un service de santé, dans l'intérêt d'en sécuriser la préservation. Une précision apportée par le Conseil d'État renforce la sécurité des données de santé des patients en élargissant le champ de compréhension et d'appréhension de celles-ci, le secret médical s'appréciant, en effet, à l'ensemble des informations, « *confié, entendu ou compris par le médecin* »[188]. La liberté et l'étendue d'écoute et de captation des données accordée au professionnel de santé, prouvent, une fois encore, l'importance de celles-ci et par là renforcent le sentiment protecteur à leurs égards.

Une lecture de l'article précitée, *in fine*, fait preuve du tour de force réalisé par le Code de la santé publique d'ériger les données de santé au même degré que la vie du patient. En effet, le respect dû au secret des informations concernant un patient équivaut au respect dû à la vie privée[189] du patient même. Si le patient ou les données de santé qui lui appartiennent sont confondus, il est normal qu'une protection accrue soit réalisée, par le patient, mais aussi par des organes extérieurs pour celui-ci. La prise en compte de l'importance des données de santé du patient se retrouve également au travers le volet pénal par la sanction encadrant le non-respect de celles-ci, une violation du secret médical étant punie d'un an d'emprisonnement et de 15 000 euros d'amende[190].

---

[187] CSP., art. L. 1110-4 *(Ord. nº 2017-31 du 12 janv. 2017, art. 5-1º)*.

[188] « *Considérant qu'aux termes de l'article L. 1110-4 du code de la santé publique (...) ; qu'aux termes de l'article R. 4127-4 du même code (...) ; que le secret institué par ces dispositions s'étend à toute information de caractère personnel confiée à un praticien par son patient ou vue, entendue ou comprise par le praticien dans le cadre de son exercice* », CE., 17 juin 2015, n° 385924.

[189] C. civ., art. 9, *préc.*

[190] C. pén., art. 226-13.

Si le patient est titulaire de la protection de ses données, celles-ci sont néanmoins encadrées par la loi et des règles de protections spécifiques qui en font, au-delà même de ce qui vient d'être énoncé des données que l'on qualifie souvent de « superprotégées » et dont, avant même la mise en place du règlement sur la protection des données, le législateur[191] avait souhaité donner une analyse plus précise. En effet les dispositions de l'article L. 1110-4-1 du Code de la santé publique mettent en œuvre un régime de protection particulière des données de santé dont l'État se veut garant[192].

Sur ce point, il est également à noter que si l'article L.1111-8 du Code de la santé publique[193] présentait une définition des données de santé, certains auteurs notent que celle-ci est modernisée[194] par le considérant 35 du Règlement général sur la protection des données personnelles qui estime que « *Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée* »[195].

La précision apportée par le règlement dépeint, une fois de plus, la jonction entre le droit médical et les données personnelles, pour autant que celles-ci n'en soient qu'accessoires.

46. A un second niveau, la donnée de santé pose également le lien de la protection de la donnée avec sa transmission à des fins de bonne médecine. En effet, la prise en charge transversale d'un patient pose souvent la question de l'échange de ses données entre les différents intervenants.

---

[191] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé (JORF n°0022 du 27 janvier 2016 texte n° 1) dite loi « Touraine ».

[192] CSP., art. L. 1110-4-1 *(L. n° 2016-41 du 26 janv. 2016, art. 96-I-2°)*.

[193] CSP., art. L. 1111-8 (*Ord. n° 2017-27 du 12 janv. 2017, art. 1er et 3, mod par Décr. n° 2018-137 du 26 févr. 2018, art. 3, en vigueur au plus tard le 1er avr. 2018*).

[194] « *Cette dernière définition* (cf. consid. 35 RGPD) *semble élargir sensiblement la définition de donnée concernant la santé puisqu'elle se réfère à « une personne » et non à un patient »*, N. Martial-Braz et J. Rochfeld, *Droit des données personnelles : les spécificités du droit français au regard du RGPD*, *Op cit*, p. 90

[195] RGPD consid. 35, *préc*.

Si l'article L. 1110-4 du Code de la santé publique[196] pose l'idée d'un équilibre entre la communication des informations médicales et le respect du secret, d'autres questions techniques se posent.

En effet, quoi que protégée par le Code pénal dans les dispositions de l'article 226-13 au titre du secret professionnel[197], la donnée de santé se doit d'être bien souvent accessible, non seulement par les professionnels de santé comme il vient d'être dit, mais aussi par les patients, titulaires de prérogatives d'accès sur leur dossier médical[198]. Ledit dossier, d'ailleurs, lui-même dématérialisé, est conservé par des tiers hébergeurs agrées auxquels s'impose le secret professionnel[199], en précisant, malgré tout, que l'hébergement des données de santé en question est réalisé en interne (par un responsable de traitement) ou de manière externalisée (auprès d'un sous-traitant).

A ce propos, l'article R.1111-8-8 du Code de la santé publique[200] précise que l'hébergement de données de santé externalisé s'effectue pour le compte d'un responsable de traitement ou pour le compte du patient lui-même, ce qui semble exclure de ce cadre législatif l'hébergement réalisé en interne par un responsable de traitement, ce dernier n'agissant pas en qualité de sous-traitant. Ainsi, ce deuxième type d'hébergement ne devrait pas faire l'objet de certification ou d'agrément tel que le prévoit pourtant le Code de la santé publique, pour autant, un tel hébergement est soumis à une obligation de sécurité des données prévues par l'article 32 du Règlement général sur la protection des données[201].

La question des hébergeurs de donnée de santé recouvre une réalité, à savoir, un souci d'évidence et de limpidité[202], ce qui pose problème quant au sort desdites données. L'enjeux est tel que le règlement européen s'immisce au soutien du Code

---

196 CSP., art. L. 1110-4, *préc.*

197 C. pén., art. 226-13, *préc*.

198 CSP., art. L. 1111-7.

199 CSP., art. L. 1111-8 et s. *(Ord. nº 2017-27 du 12 janv. 2017, art. 1er et 3, mod. par Décr. nº 2018-137 du 26 févr. 2018, art. 3, en vigueur le 1er avr. 2018)*.

200 CSP., art. R. 1111-8-8.

201 RGPD art. 32, *préc.*

202 « *Dans tous les cas, il est clair que les articles du Code de la santé publique sur la qualification d'hébergeur de donnée de santé manquent de clarté, et de cohérence avec le RGPD* », URL : https://www.village-justice.com/articles/hebergement-donnee-sante-rgpd,30355.html#XIqQuURc0u2xZ8S9.99

de la santé publique, afin de pallier certaines de ses failles pour le bien de ces informations (données de santé) dont l'importance est, pour le patient, considérable.

Il était donc essentiel de rappeler le caractère fondamental et au demeurant en lien avec la dignité de la personne qui protège l'ensemble des données médicales des personnes.

47. Aussi, puisque le « sacro-saint » secret médical s'impose inéluctablement, il apparait essentiel que le Règlement européen sur la protection des données personnelles soumette un cadre aux différents professionnels de santé afin que ces derniers assurent entière protection des différentes « données personnelles » que le patient aura alors délivrées.

Là encore, voici une illustration d'un phénomène liant un type d'obligation avec la notion de « donnée personnelle », alors que cette dernière n'est pourtant qu'un « objet » secondaire à ce contrat.

§2 Les conséquences pour le droit des obligations quand les données personnelles sont accessoires

48. Dans l'intention de déterminer les conséquences pour le droit des obligations lorsque les données personnelles en sont accessoires, il sera intéressant d'apprécier les répercussions du Règlement général relatif à la protection des données personnelles sur ces différents contrats, et par là, se poser la question de l'existence d'une protection particulière, ou non, relative aux « données personnelles ».

Pour le dire autrement, il convient de se demander en quoi la présence des « données personnelles » vient modifier l'étude classique qui peut être faite de l'objet de ces différents contrats.

49. Une modification de ces contrats est-elle nécessaire à partir du moment où la problématique des « données personnelles » s'y rattache ? Dans l'ensemble non.

Le contrat entendu au sens commun, reste contrat, le fait que des « données personnelles » y soient intégrées ne transforme pas celui-ci. Chaque contrat garde ses exigences et un cadre propre (et les dispositions du Code civil vont en ce sens). Pour autant, il est vrai que le règlement général sur la protection des données impose certaines conditions permettant ainsi de renforcer la sécurité qui entoure les « données personnelles ».

Quoi qu'il en soit, chaque obligation, précédemment visée, dont la « donnée personnelle » est accessoire, est munie d'un cadre législatif bien propre.

50. S'il apparait que la « donnée personnelle » n'est qu'accessoire, elle est pourtant déterminante et participe aux différents changements qui ont lieu quant à ces contrats.

A ce propos, plutôt que parler d'innovation, il convient de parler de rénovation ou simplement d'amélioration, le règlement européen ne modifiant pas le cadre

législatif ni la substance même de ces différents contrats. En effet, consentir à l'utilisation des « données personnelles » ne revient pas à simplement contracter. Ainsi, lorsqu'un contrat porte sur l'utilisation de « données personnelles », il existe une double approche, d'une part celle du consentement au contrat et d'autre part celle du consentement en lien avec l'utilisation des « données personnelles ».

Le droit des obligations ne se trouve pas chamboulé par la mise en œuvre du règlement cité, bien au contraire, celui-ci venant au secours des multiples obligations qui abordent la notion des « données personnelles », sans pour autant que celles-ci en soient l'élément central.

Le Règlement général sur la protection des données apporte simplement quelques outils permettant d'éduquer respectivement les contrats de sous-traitance, les contrats de travail et les contrats relatifs au droit médical, et cela, à l'égard de la protection des « données personnelles ».
Les différents acteurs que sont les organismes de traitements (pour les contrats de sous-traitance), les employeurs (pour les contrats de travail) ou encore les professionnels de santé (pour les contrats relatifs au droit médical) deviennent, au sens du présent règlement, de véritables responsables de traitements des « données personnelles », et voient alors leurs responsabilités fortement accrues.

51. Si au fond le droit des obligations, tel qu'il était, continue d'exister, ce dernier se voit renforcer, au cas par cas, dans un souci de responsabiliser les utilisateurs des « données personnelles ». Les responsables de traitements doivent pour cela user de transparence, d'efficacité et d'opacité afin d'assurer un maximum de sécurité, notion incontestable pour veiller à la protection des « données personnelles » qui sont en leurs mains.

A ce sujet, le Règlement général sur la protection des données énonce, au sein du premier point de l'article 24, que « *Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, 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. Ces mesures sont réexaminées et actualisées si nécessaire »[203].

L'article 24 s'articule donc autour de la logique de responsabilité, qui s'impose aux responsables de traitements, représentant ainsi une des lignes de conduites et l'un des moteurs du Règlement européen de protection des données. Si ce texte peut sembler contraignant pour les différents acteurs de traitements, son utilité n'est pas à remettre en question. En effet, l'objectif principal est de mettre en avant la protection des « données personnelles » et de s'assurer que les contours du Règlement sont respectés. Bien plus que le simple respect du traitement des « données personnelles », le règlement prône un certain suivi et donc une démonstration dans l'accomplissement de celui-ci.

Ce texte n'est pas sans rappeler certains principes déjà évoqués aux articles 5, 6 et 7 du présent règlement, relatifs respectivement aux traitements des données à caractère personnel, à la licéité du traitement et aux conditions applicables au consentement. Par ces nombreuses références, autour de la notion de responsabilité, le Règlement susvisé met l'accent sur l'idée qu'il entend de la responsabilité. Ce qu'il prône conduit en effet les différents acteurs qui usent des « données personnelles », tels que les responsables de traitements, à se responsabiliser. Si le Règlement européen fixe des conditions, des critères, à respecter, une logique d'autonomie s'applique car en effet, la finalité revient aux responsables de traitement puisque c'est à eux de prouver qu'ils sont conformes avec ce que le règlement détermine.

52. Ultérieurement, plus précisément avec l'article 26, le règlement général sur la protection des données apporte une nouveauté concernant les obligations générales des responsables du traitement.

Ce texte, qui relate, *in limine*, les informations suivantes « *Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les*

[203] RGPD art. 24 al. 1er, *préc.*

moyens du traitement, ils sont les responsables conjoints du traitement »[204], semble apporter une innovation par rapport au cadre juridique précédent.

Cet article, dont la finalité est, selon la formule d'un spécialiste des révolutions numériques, « *de parer toute divergence juridictionnelle et autre stratégie de ping-pong* »[205] instaure un principe de coresponsabilité, c'est-à-dire qu'il contraint les responsables de traitements à passer, entre eux, un accord afin déterminer les rôles respectifs de chacun. L'accord passé, les détails de la coresponsabilité doivent être mis à disposition et parvenir aux personnes concernées par le traitement à titre d'information. Si cette notion de coresponsabilité ou responsabilité conjointe semble, de prime abord, alambiquée, elle présente, tout compte fait, un avantage, gage de sécurité, pour les personnes concernées.

En effet la coresponsabilité concerne l'exemple type suivant à savoir, deux ou plusieurs responsables traitant une seule et même base de données. La crainte dans un tel schéma se cristallise autour de sa complexité, puisque plus il y a de responsables de traitement, plus il y a d'interlocuteurs pour la personne concernée. Celle-ci peut craindre, lorsqu'elle sollicite les différents responsables de traitement, de se retrouver isolée et sans véritable réponse, ces derniers se renvoyant l'un et l'autre la compétence, la faute, voir même la responsabilité. Voilà pourquoi un cadre précis fixe une telle possibilité à savoir la responsabilité conjointe afin de pallier à ces différentes failles. Le succès de l'obligation décrite à l'article 26 du règlement européen reposant, justement, sur un devoir partagé. En pratique, la responsabilité incombant aux responsables de traitement étant multipliée, elle ne sera que meilleure, l'union faisant la force. De plus, dans le cas où un co-responsable de traitement ne réaliserait pas la tâche qui lui incombe, l'autre responsable de traitement devra, automatiquement, le suppléer.

Cette démarche participe, une fois de plus, à la protection des dites personnes dont les données personnelles, aussi privées et sensibles soient-elles, sont

---

[204] RGPD art. 26 al. 1er, *préc.*

[205] URL : https://www.nextinpact.com/article/28047/106168-le-rgpd-explique-ligne-par-ligne-articles-24-a-50

« manipulées » et cela, dans le cas de figure présent, par deux ou plusieurs individus, entendu ici comme responsable de traitement.

La notion même de coresponsabilité découle d'un postulat simple et d'une formule quasi-mathématique. Plus les données sont sensibles et plus il y a de personnes qui agissent à leur encontre, plus il est nécessaire de renforcer la sécurité à leur égard.

Il parait donc tout à fait légitime d'apporter une sureté supplémentaire, synonyme de confiance, en obligeant les co-acteurs, qui traitent ensemble de données personnelles, à agir sur le même pied d'égalité. Pour la personne concernée par la responsabilité conjointe du traitement de ses données, l'assurance et la confiance ne peuvent qu'être accrues.

53. Pour en revenir à la problématique concernant les conséquences pour le droit des obligations quand les données personnelles sont accessoires, il convient désormais de s'intéresser à l'apport du règlement européen quant à ce sujet.

C'est l'article 82 du règlement qui, en consacrant la notion de « *droit à réparation et responsabilité* » répond à ce questionnement en disposant en son alinéa 1er 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* »[206] et en son alinéa 2 que « *Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du présent règlement. Un sous-traitant n'est 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* »[207].

[206] RGPD art. 82, al. 1er, *préc.*

[207] RGPD art. 82, al. 2, *préc.*

Pour le dire autrement et dans le but d'apporter une réponse claire, désormais avec le Règlement UE 2016/679, tout responsable de traitement ou sous-traitant, ayant violé ce dernier, sera responsable de plein droit en cas de dommage matériel ou moral.

L'article 82 alinéa 3 du Règlement européen témoigne aussi du système austère mis en place par le règlement en ce qu'il dispose que « *un responsable du traitement ou un sous-traitant est exonéré de responsabilité, au titre du paragraphe 2, s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable* »[208].
En laissant la charge de la preuve au responsable de traitement ou au sous-traitant, le texte de référence en matière de protection des données personnelles prône, là encore, la responsabilité entière de ces derniers.

Plus encore, l'article 82 alinéa 4 du Règlement général sur la protection des données traite du droit à réparation et de la responsabilité au prisme de la coresponsabilité, évoqué ci-dessus, et dispose à ce sujet que « *Lorsque plusieurs responsables du traitement ou sous-traitants ou lorsque, à la fois, un responsable du traitement et un sous-traitant participent au même traitement et, lorsque, au titre des paragraphes 2 et 3, ils sont responsables d'un dommage causé par le traitement, chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective* »[209].

54. Finalement, en étudiant les conséquences pour le droit des obligations quand les données personnelles sont accessoires, un rapprochement se manifeste entre, d'un côté, le droit des obligations et, de l'autre, le règlement général sur la protection des données, qui semble tous deux, dans leur approche, des textes voisins.

Tant en termes de responsabilité que de protections, ces deux corps de règles semblent en phase. Le Règlement de l'Union européenne s'associant aux idées

[208] RGPD art. 82, al. 3, *préc.*

[209] RGPD art. 82, al. 4, *préc.*

dégagées par le droit des obligations et le droit civil en général. Le principe de responsabilité de part et d'autre atteste de la finalité souhaitée.

En effet, l'alinéa 4 *in fine* du Règlement susvisé met en évidence la notion de « réparation effective » permettant ainsi que le dommage causé à la personne concernée soit réparé en sa « totalité ». Cette logique s'inspire bien évidement de l'éminent principe de responsabilité civile connu de tous sous l'article 1382 devenu, depuis la réforme du droit des obligations, l'article 1240 du Code civil, qui évoque en ces mots « *Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer* »[210]. Il ressort également de l'alinéa précité un autre rapprochement avec le droit civil à savoir le principe de responsabilité solidaire. Ainsi et c'est encore une garantie pour la personne concernée, la certitude que le dommage soit réparé et compensé ne peut être, avec un tel mécanisme, qu'accentuée.

Le Règlement général sur la protection des données personnelles se sert donc de ce principe et l'adapte aux données personnelles et aux acteurs qui usent de ces dernières. La finalité qui anime l'article 82 est semblable à l'esprit originel qui anime l'ensemble de ce même règlement.

La protection des données personnelles et en l'occurrence la protection des personnes concernées reste le but principal à atteindre. Le dernier alinéa permet de se convaincre de l'esprit, évoqué en amont, puisque le Règlement européen ne se satisfait pas seulement à fixer un cadre, évoquer des règles dans le but de protéger les personnes concernées, ce dernier va plus loin encore, il affirme la logique de responsabilité et de sécurité en donnant aux individus la possibilité d'exercer le droit à réparation par des actions judiciaires, et cela auprès des juridictions compétentes[211].

Une fois de plus le règlement régissant la protection des données personnelles s'attache à fixer un véritable cadre précis, mais surtout complet, toujours pour le bien des individus et pour répondre à leurs besoins.

---

[210] C. civ., art. 1240, *préc.*

[211] RGPD art. 82, al. 4, *préc.*

55. Voici donc l'état de l'avancée et les conséquences du Règlement UE 2016/679 sur le droit des obligations et plus exactement sur les contrats dont les données personnelles ne sont qu'accessoires. Si le droit des obligations n'est nullement dérangé par le souci de protection des données personnelles, il parait plus en être une inspiration permettant de défendre ces dernières.

L'analyse de la donnée personnelle entendue comme « objet » du contrat étant terminée, il sera désormais pertinent de s'intéresser aux données personnelles en tant que fondement du but contractuel

CONCLUSION DU CHAPITRE 1

Malgré l'effacement de la notion d'objet depuis la Réforme du droit des obligations, cette notion perdure. C'est ainsi qu'il est aujourd'hui possible de trouver dans la notion de donnée personnelle une représentation actuelle de l'objet du contrat.

Qu'elle soit objet principal ou objet secondaire du contrat, la particularité de la donnée personnelle implique certaines obligations, lesquelles ne bouleversent pas pour autant le droit des obligations qui semble plutôt être un atout pour la donnée personnelle.

.

Chapitre 2 : Les données personnelles en tant que fondement du but contractuel

56. Lorsque la donnée personnelle est un élément du but du contrat, terminologie nouvelle qui a remplacé la référence critiquée de la cause, la donnée doit néanmoins obéir aux exigences classiques qui étaient traditionnellement exigées, à savoir qu'elle doit tout à la fois être licite (Section 1) mais également conforme aux règles d'exigences classiques du droit commun, à commencer par l'ordre public (Section 2).

Section 1 : La licéité en tant que caractéristique commune au contrat et aux données personnelles

57. L'exigence de licéité protège et s'impose directement aux données personnelles jusqu'à en devenir une des composantes fondamentales. Son rôle est des plus importants, tant au niveau du contrat (Paragraphe 1), lorsque la donnée personnelle est l'objet du contrat, que pour l'utilisation des données personnelles, au travers un traitement ou une collecte de celles-ci (Paragraphe 2).

§1 La licéité comme aspect essentiel des données personnelles au sein du contrat

58. Comment évoquer la licéité de la « donnée personnelle » dans le contrat, sans rappeler les principes fondamentaux qui entourent la validité même du contrat ?

Depuis la réforme du droit des obligations, intervenue le 10 février 2016, l'article 1128 (nouveau) du Code civil expose à ce sujet que « *Sont nécessaires à la validité d'un contrat : 1° Le consentement des parties ; 2° Leur capacité de contracter ; 3° Un contenu licite et certain* »[212].

59. Si, comme cela avait été précédemment évoqué[213], les notions de « consentement des parties » ou leur « capacité de contracter » ne soulèvent aucune difficulté particulière, il convient, dès à présent, d'étudier, toujours sous l'angle des « données personnelles », le concept de « contenu licite et certain ».

Pour ce faire, l'article 1128 du Code civil opère un renvoi au principe du « contenu du contrat » et invite ainsi à s'intéresser à l'article 1162 du Code civil qui, dans sa rédaction, prévoit que « *Le contrat ne peut déroger à l'ordre public ni par ses*

[212] C. civ., art. 1128, *préc.*

[213] *V. supra §n°2 sur le cadre de l'étude sur les données personnelles et le contrat.*

stipulations, ni par son but, que ce dernier ait été connu ou non par toutes les parties »[214].

60. Si l'exigence de licéité qui s'impose au contrat revêt un double aspect, les stipulations du contrat, d'un côté, et le but poursuivi par les parties, de l'autre, la référence principale reste celle de l'ordre public, dont le rôle attribué à celle-ci en fait un véritable arbitre. Par une telle manœuvre, l'intention du législateur est claire, le but est d'imposer « *une hiérarchie très nette : l'ordre public prime les intérêts des contractants, même de celui qui n'entendait pas lui porter atteinte* »[215], ce qui n'est en réalité qu'une confirmation d'une jurisprudence bien établie dans ce domaine[216].

L'impératif de licéité du contrat ou licéité des prestations contractuelles s'apprécie donc, notamment par le biais de l'ordre public, pour autant, certains auteurs considèrent qu'elle amène, également, à s'intéresser aux choses et prestations qui se retrouvent dans le commerce.

L'expression contenue dans l'article 1598 du Code civil, ainsi rédigé « *Tout ce qui est dans le commerce peut être vendu lorsque des lois particulières n'en ont pas prohibé l'aliénation [217]»,* permet de traduire, de manière positive, le fait que la chose puisse faire l'objet d'un commerce juridique. En effet, la lecture de l'article 1598 du Code civil *in limine* évoque une idée dogmatique et péremptoire à savoir que « *Le principe est que tout bien, tout droit est dans le commerce* »[218]. Pour autant, puisque tout principe à ses exceptions, l'article 1598 du Code civil *in fine* n'échappe pas à cette règle en faisant état de certaines restrictions, lesquelles seront étudiées ci-après.

---

[214] C. civ., art. 1162, *préc.*

[215] N. Dissaux, *Contrat : formation – Détermination des conditions, Op. cit.*; V. déjà A. Weill, *Connaissance du motif illicite ou immoral déterminant et exercice de l'action en nullité* : in Mél. G. Marty, 1978, p. 1169.

[216] Civ. 1re, 7 oct. 1998: nº 96-14.359; D. 1998. 563, ccl. J. Sainte-Rose ; D. 1999, Somm. p. 110, obs. P. Delebecque ; JCP 1999, I, 114, § 1 s., obs. C. Jamin, et 1999, II, 10202, note M.-H Maleville ; Défrenois 1998, p. 1408, n° 138, obs. D. Mazeaud.

[217] C. civ., art. 1598.

[218] A. Bénabent, *Droit des obligations*, *Op cit*, p.148.

61. Mais avant cela, il convient d'approfondir la présente étude à l'aune du terme « commerce » présent dans l'article mentionné ci-dessus. Pour ce faire, une interrogation survient, à savoir à quel sens du mot commerce l'article fait-il référence ?

Si l'article L.121-1[219] du Code de commerce précise que « *Sont commerçants ceux qui exercent des actes de commerce et en font leur profession habituelle* », ce sont les articles L. 110-1[220] et L. 110-2[221] du même Code qui retranscrivent, par différents exemples, ce qu'il faut appréhender par « acte de commerce » au sens de la loi, sans en donner une définition générale. Plus simplement, en langage courant, le commerce représente *« une activité qui consiste à acheter et à vendre des marchandises, des denrées, des valeurs, des services, en vue de réaliser un profit »*[222]. Une telle définition, globalisée, ne semble pas avoir d'égal au sens juridique, puisqu'en effet, aussi bien, les différents dictionnaires[223] juridiques, le vocabulaire[224] juridique, ou encore, le lexique[225] juridique, ne développent ou ne font références à cette notion.

62. Aussi, puisque la notion de « commerce juridique » n'est pas dotée de définition réellement établie, en tant que telle, la signification de ce terme, de cette expression, s'apprécie au moyen de nombreuses restrictions qui composent cette dernière, permettant ainsi de la déterminer. C'est donc, au travers du concept des choses « hors commerce juridique » qu'il convient d'appréhender la notion contraire, précitée, de « commerce juridique ».

---

[219] C. com., art. L. 121-1.

[220] C. com., art. L. 110-1.

[221] C. com., art. L. 110-2.

[222] URL : https://www.dictionnaire-academie.fr/article/A9C3120

[223] Dictionnaire du vocabulaire juridique 2020, *Op cit* ; Dictionnaire juridique, Collection Paradigme, 3e édition, sous la direction de C. Puigelier.

[224] G. Cornu, *Vocabulaire juridique*, Quadrige, PUF, 12e édition mise à jour, sous la direction de l'Association H. Capitant.

[225] *Lexique des termes juridiques*, Dalloz, 26e édition, 2018-2019, sous la direction de S. Guinchard et T. Debard.

Si l'identification de ce qu'est, concrètement, le « commerce juridique » n'est pas chose aisée, l'analyse de l'expression « hors commerce » ne l'est, à son tour, pas non plus. Déjà en 1988, Loïc Cadiet estimait en ce sens, au sujet de l'article 1598 du Code civil, que « *Les choses hors du commerce appartiennent à ces catégories juridiques essentiellement marquées par la désaffection doctrinale* »[226].

Afin de résumer et d'étudier cette notion, il convient de garder à l'esprit que, relève de la catégorie des choses « hors commerce juridique » les biens et droits qui ne peuvent pas faire l'objet de contrats. Pour le dire autrement, certaines choses sont, en effet, hors commerce puisqu'elles font l'objet d'interdit. Ladite notion, ainsi appelée « commerce », doit se comprendre dans son aspect le plus vaste, puisqu'il serait bien trop réducteur de, seulement, cantonner le commerce à l'opération contractuelle de la vente.

Une autre fausse affirmation est également à éviter, dans le sens où les choses hors commerce ne sont pas uniquement les choses hors marché. En effet, le principe de gratuit permet aux choses d'échapper à tous types de relations marchandes ou commerciales, sans pour autant disparaitre du commerce juridique.

Pour résumer, « *Une chose hors le commerce est une chose qui ne peut l'objet de transaction parce que le droit juge, pour des raisons morales ou pratiques, que les choses de cette sorte ne sont pas commercialisables* » [227]. Autrement dit, la chose hors commerce est celle qui ne peut pas être l'objet d'un acte juridique, quel qu'il soit, qu'il s'agisse d'une convention ou d'un acte juridique unilatéral qu'il soit gratuit ou onéreux.

63. Voici, ci-après, quelques illustrations permettant de caractériser la distinction entre les différentes catégories qui composent le commerce juridique, en détaillant, plus particulièrement, les choses qui sont hors commerce juridique.

---

[226] L. Cadiet, Jurisclasseur Civil, 1988, n°5, art. 1598.

[227] F.-X. Testu, *Chapitre 11 : élément du contrat - Section 3 : objet du contrat* , in *Contrats d'affaires* , éd., Dalloz référence, 2010.

Dans l'intention de réaliser un inventaire, non exhaustif, des choses hors commerce, il est avant tout important de comprendre qu'une sous division existe, au sein de cette catégorie. C'est en effet ce que remarque, très justement, Grégoire Loiseau qui précise « *Dans la recherche d'une typologie des choses hors commerce, une distinction est opérée entre les choses hors commerce et celles qui sont hors du marché* »[228]. Les choses hors du commerce juridiques recouvrent alors deux réalités.

D'un côté, les choses sont hors commerce par essence ou par nature. « *La catégorie des choses hors commerce est alors essentiellement limitée à la personne humaine et à ce qui concerne la dignité de la personne humaine et du corps humain* »[229].

Tandis que d'un autre côté, les choses sont hors marché parce que la société ou l'ordre juridique en décide ainsi. « *La catégorie des choses hors du marché distingue les choses susceptibles d'appropriation qui, pour un motif juridique particulier d'ordre subjectif, en sont exclues comme, par exemple, les stupéfiants* »[230].

64. Seront qualifiées de choses hors du commerce juridique car frappées d'illicéité toutes les choses qui « *heurtent l'exigence de conformité à l'ordre public posé le nouvel article 1162 du Code civil, et sont par conséquent soumises à la même prohibition, toutes les choses frappées d'inaliénabilité en raison du caractère illicite qui toucherait leur propriété ou leur exploitation* »[231]. Il s'agit ici, de toutes substances interdites, purement et simplement, telles que la drogue. Par ailleurs, d'autres éléments, pourtant anodin, sont prohibés et ne peuvent pas être l'objet de commerce parce qu'ils sont colorés par une connotation interdite, c'est ainsi que le Code pénal[232] ou le Code rural et de la pêche maritime [233] font état d'exemples multiples à ce sujet, excluant, notamment, « *le fait de faire commerce d'un*

---

[228] G. Loiseau, *Typologie des choses hors du commerce*, RTD*Civ*., 2000, p.47.

[229] J. Lefebvre, *Leçons de droit des biens*, Éditions Ellipses, Collection « Leçons de droits », 2e édition, p. 16.

[230] *V. Supra, §n°62 sur la catégorisation de la chose hors commerce.*

[231] Y. Strickler, *Droit des biens*, Edition LGDJ, Collection « Cours », LMD 2017, p. 133.

[232] C. pén., art. 227-24.

[233] C. rur., art. L. 211-15.

message de caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine »[234], ou encore, *« l'acquisition, la cession à titre gratuit ou onéreux, l'importation et l'introduction sur le territoire national des chiens de la première catégorie, c'est-à-dire les chiens d'attaque »*[235].

Pour résumer l'étude présente et revenir sur l'idée principale, à savoir la question des données personnelles et l'exigence de licéité, il convient donc de retenir que sont hors du commerce les divers objets d'origine illicite tels que, des produits dangereux[236], des objets de contrefaçons[237], des tombeaux[238], des souvenirs de famille[239] ou bien encore des fichiers de clientèles non déclarés, cette dernière jurisprudence étant, plus amplement, détaillée ci-dessous.

65. A ce sujet, c'est la jurisprudence qui a réalisé le travail de confronter la notion de « fichier informatique », à travers de laquelle il convient d'entendre celle de « donnée personnelle », avec la licéité, au sens de contenu du contrat.

Par un arrêt du 25 juin 2013, rendu par la Chambre commerciale, précédemment exposé, les Hauts magistrats de la Cour de cassation ont dégagé le principe selon lequel « *Tout fichier informatisé contenant des données à caractère personnel doit faire l'objet d'une déclaration auprès de la CNIL ; la vente d'un tel fichier, qui, n'ayant pas été déclaré, n'était pas dans le commerce, a un objet illicite* »[240].

La censure opérée par la chambre commerciale de la Cour de cassation, au double visa des articles 1128 du Code civil et 22 de la Loi du 6 janvier 1978, fait entrer le fichier informatisé contenant des données à caractère personnel non déclarées à la Commission nationale de l'informatique et des libertés dans la catégorie des

---

234 CJCE., 14 oct. 2004, aff. C-36/02, *Omega c/ Oberbürgermeinsterin der Bundesstadt Bonn, BICC n°611* du 15 janv. 2005.

235 J.-M. Pontier, *Du danger présenté par certains chiens et des moyens d'y remédier*, *JCPA 2008*, act 608.

236 Cass. com., 16 mai 2006, Bull civ., IV, n°124 (produits périmés).

237 Cass. com., 26 octobre 1999, Bull civ., IV, n°185, ou encore, Cass., 24 septembre 2003, Bull. civ., IV, n°147.

238 Cass. civ., 23 mars 1977 et 13 mai 1980, *JCP* 1997.II.18658 et 1980.II.19439, concl. GULPHE.

239 Cass. civ.,29 mars 1995, *JCP* 1995.II.22477, puis 12 novembre 1998, *D. 1999.624*.

240 Cass. com., 25 juin 2013, n° 12-17.037, *préc.*

« choses hors du commerce ». La solution rendue par la chambre commerciale de la Cour de cassation est l'illustration d'une conception élargie de la catégorie des « hors du commerce » et l'article 1128 du Code civil s'enrichit des fichiers à caractère personnel non déclarés à ladite Commission.

Si le 25 juin 2013, le débat est centré autour de la perception des fichiers informatiques contenant des « données personnelles », cette préoccupation était timidement semblable en 1978, mais ne se cantonnait qu'aux « fichiers informatiques » sans y joindre la notion de « donnée personnelle ».

En effet, l'article 1er de la loi 6 janvier 1978, ne faisait lui, en son temps, que règlementer la validité de la question de l'informatique dans sa globalité puisqu'il énonçait que « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. 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* »[241].

C'est donc grâce à la jurisprudence et par la pratique que les prémices autour de la question de la licéité de la donnée personnelle dans le contrat apparaissent.

66. Originellement, en droit français, la donnée à caractère personnel, correspond, selon l'article 2 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à « *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* »[242]. Si cette définition semble succincte, il ne faut pas oublier qu'au moment de son élaboration, la loi du 6 janvier 1978 avait pour ambition première de protéger les citoyens contre les intrusions des administrations étatiques. Ce n'est qu'en 1995 que la directive européenne donne une autre dimension aux données personnelles en préservant les intérêts de celles-ci et cela contre les grands acteurs économiques. En effet, la révolution numérique, la

[241] Art. 1er, Loi n° 78-17 du 6 janvier 1978, *préc.*

[242] Art. 2, Loi n° 78-17 du 6 janvier 1978, *préc.*

marchandisation et l'internationalisation des données sont autant de dangers pour les données personnelles et marquent le passage de préoccupations des données du volet public à privé. Aujourd'hui, voilà pourquoi la définition posée par le Règlement européen, qui s'inspire d'une longue tradition protectrice, semble aboutie, complétée par de nouvelles préoccupations en lien avec son époque.

Voici donc, en l'état, le cadre juridique et la définition légale qui dessinent la notion de « donnée personnelle ». Cette définition extensive permet d'enrôler en son sillage une multitude de représentations de ce qu'est, en réalité, une « donnée personnelle ».

Ainsi, peut être considéré comme une « donnée personnelle », un nom, une photographie, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, une adresse IP, un identifiant, un enregistrement vocal, un groupe sanguin ou encore une date ou un lieu de naissance…

En résumé, est une donnée à caractère personnel toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement, et ce, que ces informations soient confidentielles ou publiques.

67. Si le concept de « donnée personnelle » semble précis, quelques restrictions, puis précisions, sont à énoncer.

En premier lieu, il convient de noter qu'une donnée à caractère personnel ne peut concerner que les personnes physiques. En effet, sont exclues du champ d'application de cette notion les informations relatives aux personnes morales, qui ne sont-elles, pas protégées.

Ensuite, il est important d'ajouter, suite à cette définition légale, que selon la Commission nationale de l'informatique et des libertés pour que les données personnelles « *ne soient plus considérées comme personnelles, elles doivent être rendues anonymes de manière à rendre impossible toute identification de la*

personne concernée »[243]. La Commission ajoutant, enfin, à titre de mise en garde, que dans le but d'identifier une personne, les données restent personnelles même si ces dernières sont captées par « *recoupement de plusieurs informations ou par l'utilisation de moyens techniques divers* »[244].

68. Dans l'intention d'aboutir à cette analyse complète du principe de licéité de la « donnée personnelle » au sein du contrat, il convient d'étudier ledit élément au prisme des articles liés aux droits de la « personnalité de la personne », que sont principalement les articles 9 et 16 du Code civil. Si l'article 1er de la loi informatique et libertés mentionne que « *Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant* »[245], quid de la licéité de la « donnée personnelle » en droit civil français ?

L'article 9 du Code civil, en ce qu'il fait rejaillir ce principe inébranlable selon lequel « *Chacun a droit au respect de sa vie privée* »[246] et les différentes jurisprudences afférentes à celui-ci, laissent à penser que le législateur en 1804 avait déjà posé les bases de ce que le règlement européen viendra poursuivre en 2016. Pourtant, si une telle protection de la vie privée a été affirmée par la Déclaration universelle des droits de l'homme des Nations unies[247] dès 1948, il a été nécessaire d'attendre jusqu'en 1970 pour que ce principe soit, finalement, intégré au sein du Code civil. Aussi dès sa conception, ou plutôt son introduction, en tant que principe juridique législatif, la notion de droit au respect de la vie privée semble complice avec celle de données personnelles. Si les premières représentations des données personnelles, rudimentaires et primitives, avaient pour gardien l'article 9 du Code civil, le développement du secteur privé a permis l'émergence de la Loi informatique et libertés du 6 janvier 1978 comme soutient aux nouvelles illustrations de celles-ci, et c'est aujourd'hui le règlement UE

---

[243] URL : https://www.cnil.fr/fr/cnil-direct/question/une-donnee-caractere-personnel-cest-quoi

[244] *Ibid.*

[245] Art. 1er, Loi n°78-17 du 6 janvier 1978, *préc.*

[246] C. civ., art. 9, *préc.*

[247] « *Nul ne sera l'objet d'immixtions arbitraire dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* », Art. 12, DUDH 1948.

2016/679, adapté à la situation et à l'environnement actuel, qui représente l'arme ultime au service des données personnelles dans leur version (technologique, numérique) la plus aboutie.

69. Plusieurs décisions rendues à l'aune de cet article, dont voici les illustrations, mettent en lumière la protection et l'importance de la licéité des « données personnelles », tel qu'elles sont perçues par le Règlement général sur la protection des données, dans le contrat.

En effet, bon nombre d'informations ou, pour parler au gout du jour, de « données personnelles » sont protégées par les juridictions de droit commun. C'est le cas par exemple pour la 1ère Chambre civile qui énonçait, déjà, dans une décision en date du 5 juin 1996, que « *la seule constatation de l'atteinte à la vie privée ouvre droit à réparation* »[248].

Quelques années plus tard, et pour rentrer dans le vif du sujet, le Conseil constitutionnel estimait au sujet des collectes d'informations que « *La collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif* »[249].

Plus marginalement, la Cour d'appel de Pau dans une décision du 22 janvier 2001 déclarait que *« La voix constitue l'un des attributs de la personnalité et peut bénéficier de la protection instituée par l'article 9 dans la mesure ou une voix caractéristique peut être rattachée à une personne identifiable* »[250]. Aussi, la Cour de cassation précisait-elle au sujet d'une adresse de domicile que « *La publication dans la presse de la résidence d'une personne, accompagnée du nom du propriétaire et de la localisation précise, constitue une atteinte au respect de la vie privée* »[251]. Enfin, le Tribunal correctionnel de Briey en date du 15 septembre 1992 rendait la décision suivante, « *La divulgation d'un numéro de téléphone a pour effet de porter atteinte à l'intimité de la vie privée de son titulaire* »[252].

---

[248] Cass. civ. 1ere, 5 novembre 1996, n°94-14.798, Bull 1996 I n°378 p. 265.

[249] Cons. const., 13 mars 2014, n° 2014-690 DC.

[250] CA., Pau, 22 janvier 2001.

[251] Cass. civ. 2e, 5 juin 2003, n°02-12.853.

[252] T. corr., Briey, 15 septembre 1992, Gaz. Pal. 1993. 1. 201.

Il est évident que ces différents exemples ne sont pas sans rappeler la logique du Règlement européen, celui de protéger les « données personnelles ». Voici en effet qu'à la lumière de l'article 9 du Code civil, les « données personnelles » ou timidement appelées par le passé « informations propres à la vie privée » étaient déjà surveillées, chaque individu étant le propriétaire exclusif des « données » attachées à sa personne.

Une dernière décision rendue par la Cour de cassation le 17 mars 2016 disposant 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* »[253], permet de rapprocher le Code civil et les différentes juridictions françaises d'avec le Règlement UE 2016/679, ce dernier évoquant aussi le fait que seules les « données personnelles » des personnes physiques sont protégées.

70. Plus encore, la licéité de la donnée personnelle dans le contrat est à rapprocher des principes fondamentaux posés par l'article 16 du Code civil. La jurisprudence, a d'ailleurs eu l'occasion, au visa de l'article précédemment évoqué, de préciser ce point en consacrant l'idée que « *La sauvegarde de la dignité de la personne humaine contre toute forme d'asservissement et de dégradation est un principe à valeur constitutionnelle* »[254]. En effet, comme il a déjà été précisé[255], le caractère éminemment fondamental des dispositions issues de l'article 16 du Code civil tend à suggérer que la protection par le biais de la dignité se doit d'être aussi large que possible.

C'est pourquoi, il a rapidement été question de faire supporter la protection issue de ce texte sur tout ce qui relève du volet moral de la personne, à commencer par ce qui relève de son intimité ou de son image[256]. C'est donc tout naturellement que, par la suite, le principe sera étendu aux « données personnelles ».

---

[253] Cass. civ. 1ère, 17 mars 2016, n°15-14.072.

[254] Cons. const., 27 juillet 1994, *préc.*

[255] *V. supra, §n°9.*

[256] V. Civ. 1re, 20 déc. 2000, *préc.*

En effet, un arrêt de la Cour européenne des droits de l'homme du 10 octobre 2006 précise, qu'il y a « *Violation de l'art. 8 Conv. EDH, compte tenu du rôle fondamental de la protection des données personnelles, en cas de reproduction par le juge, dans les motifs de la décision, d'extraits d'une pièce médicale confidentielle* »[257].

Cette extension n'a rien que de très logique, les « données personnelles » sont des informations si intimes, si personnelles qu'elles représentent une partie de la vie privée de la personne concernée et cette même vie privée est une déclinaison du droit à la dignité de la personne humaine. La conformité de la « donnée personnelle » avec le respect de l'être humain et la dignité est une constante non négligeable. En effet, le souci de préserver la dignité humaine s'applique aux « données personnelles », ces dernières étant des informations qui représentent, à elles seules, des fragments de la personnalité humaine.

[257] CEDH., sect. II, 10 octobre 2006, *préc.*

§2 La licéité, qualité élémentaire du traitement des données personnelles

71. Bien plus que d'être seulement confronté aux données personnelles, lorsque ces dernières sont directement liées au contrat, l'exigence de licéité se retrouve également en présence du processus de collecte de données à caractère personnel ou, pour le dire autrement, au traitement de celles-ci.

L'exigence de licéité s'exprime par une conformité, sinon une soumission aux règles établies. En effet, ce sont les normes supérieures, qu'importe leurs formes, traité, règlement, loi, usages, coutumes, morales, religion, ou autres, qui vont autoriser, permettre l'émergence d'une action. En l'occurrence, concernant la licéité du traitement de données personnelles, celle-ci est encadrée par le terme de « privacy by design » lequel impose des conditions d'application strictes et cumulatives dont le but est d'« *assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée* »[258].

72. L'entreprise qui consiste à s'intéresser, précisément, à la condition de licéité et l'impact de celle-ci par rapport aux données personnelles ou au traitement s'applique, aujourd'hui, dans le règlement général sur la protection des données, lequel est entré en application en 2018. Pour autant, cette manœuvre ne date pas d'hier, ce qui en démontre l'importance.

Cet objectif existait déjà au moment de l'arrivée de la loi du 6 aout 2004[259] relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, modifiant la loi du 6 janvier 1978[260], puisque comme l'énonçait Nathalie Mallet-Poujol « *Une des grandes nouveautés tient à*

[258] RGPD art. 25, *préc.*

[259] Loi n°2004-801 du 6 aout 2004, *préc.*

[260] Loi n° 78-17 du 6 janvier 1978, *préc.*

l'introduction de conditions de licéité du traitement »[261]. Cette réforme dont la vocation était de transposer en droit français les dispositions de la directive du 24 octobre 1995[262], elle-même, à son tour, remplacée par le règlement européen, objet de l'étude en question, était le moyen d'apporter quelques exigences supplémentaires pour conforter la protection relative aux données personnelles, notamment par l'intronisation de conditions de licéité concernant le traitement de celles-ci. En se réjouissant d'un tel apport, l'auteure précitée prouve et démontre un défaut de l'ancienne loi informatique et libertés, ancêtre du règlement UE 2017/679, à savoir que celle-ci ne faisait ni état, ni mention d'une quelconque exigence de licéité. Et pour cause, cette absence, remarquée, étant, notamment, admise par le fait que les technologies de traitement des données personnelles n'étant anciennement pas aussi complexes qu'aujourd'hui, ce qui justifie le besoin d'une telle réforme.

En pratique, si l'ancienne loi informatiques et libertés n'assurait que peu de protection concernant la licéité du traitement des données à caractère personnel[263], la réforme de 2004 a permis une évolution[264] sans précédent à ce sujet, à travers certaines modifications érigeant notamment un chapitre propre aux conditions de licéité dudit traitement[265].

73. L'introduction d'une attention particulière portée à la licéité des traitements des données personnelles est fort heureusement bienvenue et l'esprit du Règlement général sur la protection des données est de poursuivre cette démarche. C'est pourquoi, il convient, désormais, au prisme de ce dernier, de se pencher sur l'étude

---

[261] Pour un commentaire, voir « La réforme de la loi ''informatique et libertés'' », N. Mallet-Poujol, chargée de recherches au CNRS, *Revue française d'administration publique*, n°89, janvier-mars 1999, p. 49-62.

[262] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, *préc.*

[263] « *La seule disposition protectrice résultait du droit d'opposition pour raison légitime prévu à l'ancien article 26, ou encore de dispositions particulières, tel le consentement préalable au traitement de données dites « sensibles » (ancien article 31)* », M-L. Laffaire, *Protection des données à caractère personnel : Tout sur la nouvelle loi ''informatiques et libertés''*, Éditions d'Organisations, p. 63.

[264] « *Rappelons que la loi du 6 janvier 1978 (ancienne) ne prévoyait pas les conditions de licéité du traitement. Désormais, la mise en œuvre d'un traitement doit se justifier par l'un des cas visés par la loi (article 7)* », M-L. Laffaire, *Protection des données à caractère personnel : Tout sur la nouvelle loi ''informatiques et libertés''*, *Ibid*, p. 63.

[265] Art. 6 à 10, Modifié par la Loi n°2004-801 du 6 aout 2004 – art. 2 () JORF 7 aout 2004.

de la licéité en tant que qualité élémentaire du traitement des données personnelles.

Pour ce faire, le règlement européen impose l'idée suivante, à savoir que pour mettre en application un traitement de données personnelles, celui-ci doit, obligatoirement, se fonder sur l'une « bases légales »[266] prévues à cet effet, ainsi, la licéité du traitement, en question, est conditionnée par six impératifs détaillés au sein de l'article 6 (1.)[267], « *Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ; b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ; c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ; e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant* .

74. L'évolution est notable, l'exigence de licéité est clairement affichée par le règlement UE 2016/679, spécifiquement dans l'intitulé du texte en question. En cas d'entrave, un responsable de traitement ne peut pas dédouaner sa responsabilité par une quelconque méconnaissance des règles en vigueur, tout en sachant qu'en imposant un cadre, une liste de possibilités, propice, ou non, au traitement de données personnelles le présent règlement assoit sa position,

---

[266] « *La base légale d'un traitement est ce qui autorise légalement sa mise en œuvre, ce qui donne le droit à un organisme de traiter des données à caractère personnel. On peut également parler de « fondement juridique » ou de « base juridique » du traitement* », URL : https://www.cnil.fr/fr/la-liceite-du-traitement-lessentiel-sur-les-bases-legales-prevues-par-le-rgpd

[267] RGPD art. 6 (1.), *préc.*

légitime, une fois de plus, son objectif de protection des données personnelles et des personnes concernées et soumet à sa bonne volonté ou plutôt à ses règles (ce qui fait écho à la définition du terme licéité) toute action de responsables de traitement. Une telle manœuvre est également renforcée par le fait que l'article 6, consacré au principe de licéité du traitement, soit positionné en début de règlement, ce qui démontre l'importance accordée à celui-ci puisqu'il pose les bases relatives à tout traitement de données. Mais alors, que recouvre la notion de cesdites bases légales ?

Le premier fondement autorisant le traitement de données s'apprécie à travers le consentement de la personne concernée, lui-même conditionné[268], en précisant toutefois que le consentement parfait, c'est-à-dire lorsqu'il répond à toutes les attentes, « *n'a pas toute puissance* »[269] car il ne permet pas de valider un traitement ne satisfaisant pas l'exigence de proportionnalité.

Lorsque le traitement de données personnelles est relatif à l'exécution d'un contrat, la seule présence du contrat ne suffit pas, en lui-même, une exigence supplémentaire de nécessité[270] s'ajoutant pour plus de sécurité.

Concernant le recours au troisième fondement, c'est-à-dire le traitement nécessaire à l'exécution d'une obligation légale, il n'est possible que si deux critères cumulatifs sont respectés[271], ce qui permet, une fois encore, plus de contrôle de l'exigence de licéité du traitement.

Quant au traitement fondé sur l'exécution d'une mission de service ou d'intérêt public, s'il peut être utilisé par un responsable de traitement du secteur public ou privé, sans différenciation, le responsable en question doit toutefois être investi d'une mission de service public et le traitement concerné rendu nécessaire par l'exécution de cette mission.

---

[268] « *Un consentement valable implique une manifestation de volonté libre, spécifique, éclairée et univoque* », URL : https://www.village-justice.com/articles/consentement-valide-sens-rgpd,30428.html

[269] M. Bourgeois, *Droit de la donnée : Principes théoriques et approche pratique*, Éditions LexisNexis, p. 60.

[270] « *Les textes exigent que le traitement soit nécessaire* », M. Bourgeois, *Droit de la donnée : Principes théoriques et approche pratique*, *Ibid*, p. 60.

[271] « *L'opération doit être de source effectivement légale et l'obligation légale doit être explicite quant à la nécessité de réaliser un traitement* », M. Bourgeois, *Droit de la donnée : Principes théoriques et approche pratique*, *Ibid*, p. 60.

Le fondement propre à l'intérêt légitime ne s'apprécie pas seul et doit être appliqué uniquement s'il ne méconnait pas « *les intérêts ou les libertés et droits fondamentaux* ». Cette exigence impose, selon le Groupe de travail Article 29, une « mise en balance » entre les intérêts respectifs du responsable du traitement et ceux de la personne concernée.

Le dernier fondement autorisant le traitement de données concerne celui nécessaire à la sauvegarde de la vie de la personne concernée et doit être, pour résumer, limité ou mis en relation avec des considérations « de vie ou de mort ». Ce fondement est une reprise de la loi informatique et libertés tout en élargissant, sensiblement, sa formulation, toujours dans un souci de clarté, donc de sécurité.

Afin de parfaire l'analyse de l'apport de l'article 6 (1.) du présent règlement, il convient d'ajouter qu'un traitement de données déterminé doit correspondre à une seule base légale[272]. Cette précision permet de limiter les dérives quant au traitement de données qui doivent correspondre et être spécifiques à une seule finalité, toujours dans un souci de conformité.

75. Il ressort de chaque fondement, précité, une complexité, gage de sécurité. En effet, derrière chaque exigence rendant le traitement de données personnelles licite, se trouvent plusieurs nouvelles conditions qui s'ajoutent dans un besoin de maitrise. Pour être licite, un traitement de données devra se conformer, non seulement aux principales réclamations du règlement général sur la protection des données, mais aussi, sur une multitude de revendications supplémentaires propice à chaque base légale. Si le traitement en question est en harmonie avec ces différentes étapes, alors, il sera licite, autorisé et pleinement accepté.

Tous ces éléments permettent de démontrer l'importance de la licéité, qualité élémentaire du traitement des données personnelles. Il parait donc important de saluer les différentes prises de conscience, ainsi que les travaux successifs entrepris à son égard. Si cette condition était, à tort, oubliée par la loi originelle informatiques et libertés de 1978, tant la réforme intervenue en 2004, que le

---

[272] « *Il n'est pas possible de « cumuler » des bases légales pour une même finalité : il faut en choisir une seule » parmi les six catégories (…). Toutefois, lorsqu'un même traitement de données poursuit plusieurs finalités, c'est à dire plusieurs objectifs, une base légale doit être définie pour chacune de ces finalités »,* URL : https://www.delsolavocats.com/Comment-determiner-les-bases-legales-de-ses-traitements

Règlement européen mis en place en 2018, ont permis d'introduire cette exigence de licéité et de l'élever afin d'accroitre la protection des données personnelles, mais aussi et surtout des personnes concernées par l'utilisation, donc le traitement de celles-ci.

Toujours, dans ce souci d'étudier les données personnelles en tant que fondement du but contractuel, il convient, dès à présent, de confronter ces données aux règles d'exigence classiques du droit commun, notamment à l'ordre public et aux bonnes mœurs pour s'assurer de la conformité de ces dernières.

Section 2 : Les données personnelles en conformité aux exigences du droit commun

76. La conformité des données personnelles aux exigences du droit commun se caractérise par la conformité de celles-ci à l'ordre public (Paragraphe 1) et aux bonnes mœurs (Paragraphe 2).

§1 La conformité des données personnelles et de leur utilisation à l'ordre public

77. L'utilisation des « données personnelles » qui résulterait d'un contrat serait, en principe, naturellement libre, mais toute liberté a ses limites comme l'exprime l'article 1102 du Code civil qui énonce en ce sens que « *La liberté contractuelle ne permet pas de déroger aux règles qui intéressent l'ordre public* »[273].

Il ne sera, pour étoffer ce raisonnement, pas utile d'exprimer, à nouveau, l'article 1162 du Code civil, ce dernier inscrivant, encore une fois, le contenu du contrat sous l'égérie du respect à l'ordre public.

Le contrat est cantonné à se conformer à l'ordre public, non seulement en raison de ce texte, mais tout simplement en application du principe général[274] posé par l'article 6 du Code civil. Pour évoquer la proximité et l'interaction entre les notions de contrat et celle d'ordre public et surtout dans le but de démontrer l'influence de l'une sur l'autre, il faut savoir que « *le rôle de l'ordre public en droit des contrats est important puisque c'est un instrument limitant la liberté contractuelle* »[275]. Cette récente pensée, semble directement marquée par certaines réflexions, plus anciennes, d'auteurs à ce sujet. Tel est, notamment, le

---

[273] C. civ., art. 1102 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

[274] « *On ne peut déroger, par des conventions particulières, aux lois qui intéressent l'ordre public et les bonnes mœurs* », C. civ., art. 6.

[275] A. Danis-Fatôme, *Ordre public et protection des données à caractère personnel*, AJ contrat 2019, p. 366.

cas, par exemple, de Carbonnier, lui, qui qualifiait, déjà en 1996, l'ordre public comme « *un éternel empêcheur de contracter en tête à* tête »[276].

Aussi, bien que la volonté des contractants représente, aux côtés de la loi, une véritable source d'obligation, elle n'emporte pas toute puissance puisqu'elle est forcément encadrée. Si le principe d'autonomie de la volonté permet aux parties de donner vie à un contrat selon leurs propres choix, la liberté contractuelle accordée à ces derniers ne doit pas pour autant être synonyme de caprices. En ce sens, l'ordre public est un garde-fou contractuel qui limite, considérablement, la marge de manœuvre destinée aux parties. La légitimité et le rayonnement de ce principe tiennent au fait que son périmètre varie selon les époques et les circonstances auxquelles il s'adapte[277].

78. L'ordre public est une notion interventionniste dont la mission est d'accompagner, d'encadrer et bonifier le contrat. En effet, tout contrat qui respecte ce principe peut librement s'épanouir. Si l'importance de l'ordre public, lorsque celui-ci est rattaché au contrat ne fait pas de doute, qu'en est-il à propos des données personnelles ? Quid des données personnelles quand celles-ci reposent sur un contrat dont l'unique but est la collecte ou le traitement de ces informations intimes et privées ?

Aussi, qu'en est-il de l'utilisation des « données personnelles » ? Comment être certain, pour un particulier, que sa vie privée, sa dignité, ses informations intimes, en bref ses « données personnelles » ne seront pas utilisées dans un but qui outrepasserait le cadre normal, celui de l'ordre public ?

Si le souci, majeur, du Règlement général sur la protection des données est réputé être la « protection des données personnelles », quelques craintes peuvent apparaitre, puisque comme tout un chacun le sait, le risque zéro n'existant pas !

79. Certaines déviances dans l'utilisation des « données personnelles » sont donc à émettre et sont, de ce fait, à confronter à l'ordre public. Plusieurs craintes sont

---

[276] J. Carbonnier*, « Exorde »* dans T. Revet*, L'ordre public à la fin du XX*e *siècle*, Dalloz, 1996, p. 1.

[277] *« L'ordre public est une notion souple »,* F. Terré, Ph. Simler, Y. Lequette, *Droit civil : les obligations*, Dalloz, 11eme édition, « précis », p. 381.

envisageables concernant la récupération et l'utilisation de « données personnelles » des personnes concernées et ce sans leur accord, ce qui constitue un véritable faute, passible de sanctions sévères.

La plus grande crainte, qui est la première étape d'une intention malveillante, est l'interception par un tiers ou le piratage informatique et la revente des « données personnelles ». Vient ensuite le fichage des « données personnelles » par des algorithmes et par l'envoi de publicités ciblées en fonction des « données personnelles » frauduleusement recueillies. En tout état de cause, l'utilisation malhonnête de « données personnelles » peut entrainer, usurpation de l'identité des personnes concernées, risque de fraude à la carte bancaire ou carte de paiement, risque lié à la publication à l'insu des personnes concernées de propos, vidéos, photos ou documents, utilisation des données à des fins commerciales ou publicitaires ou encore risque de surveillance ou d'espionnage.

80. Mais alors, qu'est-ce que l'ordre public ? Si cette notion est comprise, entendue, respectée et imaginée par l'ensemble du monde juridique et plus timidement par la population de quidam, elle semble néanmoins difficilement concrète et tangible. A ce propos, outre Jacques Ghestin qui précise que « *Le caractère flou de la notion d'ordre public conduit à la faire entrer dans la catégorie des standards, ces notions indéterminées* »[278], Serge Braudo estime, à son tour, « *Il y a peu de notions juridiques qui soient aussi difficiles à définir que celle d'''ordre public''* »[279].

Ce ressenti relève du fait que l'ordre public est une notion imperceptible, ce qui ne permet pas de représentation concrète des standards qu'elle impose, mais qui plus est, c'est une notion qui abrite bon nombre de critères, de normes, tel l'intérêt général, l'impérativité des normes, les moyens d'ordre public, mais également des considérations plus sociétales tel que la paix sociale, l'ordre, la sécurité publique, la tranquillité et même la morale. En pratique, si la représentation matérielle de l'ordre public est « laborieuse », du fait de ses innombrables personnalités, ce qui

[278] J. Ghestin, *L'ordre public, notion à contenu variable, en droit privé français*, *in* Les notions à contenu variable en droit, Trav. du centre national de recherches de logique, Bruxelles, 1984, p. 77.

[279] URL : https://www.dictionnaire-juridique.com/definition/ordre-public.php

a priori semble être un défaut peut, toutefois, s'analyser en un atout, gage de sécurité tant les critères relatifs au contrôle de l'ordre public sont divers et variés.

La formule, hautement imagée, d'un juge anglais, rendue célèbre par la thèse de Malaurie, permet de se rendre compte du caractère alambiqué de l'ordre public, celui-ci estimant, à juste titre, que « *S'intéresser à l'ordre public, c'est enfourcher un cheval fougueux* »[280]. Cette expression caractérise le dynamisme dont fait preuve la notion d'ordre public puisque si elle n'est pas strictement définie, elle fait preuve de malléabilité lui permettant de s'accoutumer des évolutions politiques, économiques ou sociales. L'ordre public est donc le reflet juridique d'une société, pour un instant, un moment donné, alors que cette société est en perpétuelle mutation.

Difficilement déterminable, une définition imaginée par Carbonnier[281] permet, pourtant, de répondre à la question posée précédemment, ce dernier estimant ainsi que l'ordre public renvoie à « *l'idée générale d'une suprématie de la collectivité sur l'individu* », ajoutant de plus que, l'ordre public « *exprime le vouloir-vivre de la nation qui menacerait certaines initiatives individuelles en forme de contrats* ».Plus simplement, il sera question de définir l'ordre public comme le caractère de tout ce qui s'impose pour des raisons de moralité ou de sécurité impérative dans les rapports sociaux. Le caractère fondamental de ce que l'on vise à travers les données justifie donc que pour d'évidentes questions d'impératif sécuritaire, celles-ci relèvent de l'ordre public.

81. Dès lors, l'analyse visant à rapprocher l'utilisation des « données personnelles » avec l'ordre public ne peut pas se faire sans évoquer l'article 16 du Code civil, lui qui semble être gage de sécurité puisqu'il dispose 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* »[282]. Mais est-il réellement

[280] Juge Borrough, *Richardson v. Mellish* (1824), 2 Bing, 252, cite par P. Malaurie, dans sa thèse *Les contrats contraires à l'OP, Étude de droit civil comparé : France, Angleterre, URSS*, th. Paris, 1953, n°1, p. 1.

[281] J. Carbonnier, *Droit civil : les biens, les obligations*, PUF, 2004, n°984, p. 2037.

[282] C. civ., art. 16 (Loi n°94-653 du 29 juillet 1994 – art. 2 JORF 30 juillet 1994).

protecteur pour les données à caractère personnel ? Voilà le véritable questionnement et ce qui entoure les craintes relatives à l'utilisation des données personnelles.

Et si l'utilisation des « données personnelles » aurait pour finalité des activités contraires à la protection du genre humain, ou encore, si la seule motivation de l'utilisation des « données personnelles » serait aux antipodes des éléments caractéristiques d'une personne, alors qu'en serait-il ?

Sans donner de réponse trop hâtive, il est obligatoire et logique de rappeler que le droit à la dignité est un principe à valeur constitutionnelle. Dire cela c'est, d'ores et déjà, donner une solution, les « données personnelles », en tant qu'informations intimes d'une personne, sont en effet protégées par un organe aussi important que le Conseil constitutionnel, celui-ci déclarant dans une décision, rendue le 27 juillet 1994, que « *La sauvegarde de la dignité de la personne humaine contre toute forme d'asservissement et de dégradation est un principe à valeur constitutionnelle* »[283].

Analyser cela reviendrait logiquement à faire un parallèle entre « données personnelles » et dignité humaine, il est donc certain que le droit commun est suffisamment armé dans le but de rendre conforme l'utilisation des « données personnelles » à l'ordre public. En ce sens, par une décision rendue le 25 novembre 2008, la CEDH donnait « *Obligation pour le droit interne de garantir la confidentialité des informations concernant des patients* »[284].

Dés 2008, le cadre était donc fixé et l'utilisation des « données personnelles », tel qu'entendu à cette époque, était donc surveillée.

82. Il parait désormais important de s'intéresser, dans l'idée de confronter la conformité des données personnelles et de leur utilisation à l'ordre public, à un sujet d'actualité. L'affaire en question qui monopolise, à tort ou à raison selon ses opinions, l'actualité médiatique et politique est celle concernant la récente proposition de loi relative à la sécurité globale[285].

---

[283] Cons. const., 27 juillet 1994, *préc.*

[284] CEDH., 25 novembre 2008, *A. et B. c/ Lituanie*, n°36919/02.

[285] Proposition de loi n° 3452 relative à la sécurité globale, Enregistrée à la Présidence de l'Assemblée nationale le 20 octobre 2020.

Avant de comprendre en quoi cette proposition de loi intéresse particulièrement les données personnelles et l'ordre public, il convient d'en présenter les objectifs, non sans quelques rebondissements.

Déposée au Parlement depuis le 20 octobre 2020, la proposition de loi précitée, renommée depuis « *proposition de loi pour une sécurité globale préservant les libertés* », s'inscrit dans une volonté de sécurité[286], voulue au plus haut sommet de l'État[287], afin de répondre à l'émergence de violences en tout genre (délinquance, crises sociales, attentats et terrorisme) ayant touché le pays français. A travers cette logique de sécurité, la présente proposition de loi met en avant deux axes de travail[288] c'est à dire, la sécurité des populations et la sécurité des forces d'État, à savoir les policiers municipaux et nationaux, les militaires (incluant les gendarmes), et le secteur de la sécurité privée. Voilà, en somme, ce que recouvre l'intitulé « sécurité globale ».

Mais alors, en quoi cette proposition de loi intéresse les données personnelles ? Ce sont les différentes thématiques abordées par cette proposition de loi qui répondent à cette interrogation. En effet, cette dernière, dont l'objectif est de renforcer les pouvoirs de police, aborde pour ce faire des sujets tel que l'accès aux images des caméra-piétons, la captation d'images par les drones ou encore la diffusion de l'image même des policiers, qui ne sont en réalité que des fragments de vie privée synonymes de données personnelles comme l'énonce, pour

---

[286] *« La proposition de loi porte sur les outils de surveillance (caméras piétons, drones…) et la protection des forces de l'ordre (nouveau délit de provocation à l'identification d'un policier, pénalisation de l'achat de mortiers d'artifice…). Elle renforce, par ailleurs, les polices municipales et encadre les sociétés de sécurité privées »,* URL : https://www.vie-publique.fr/loi/277157-loi-pour-une-securite-globale-preservant-les-libertes

[287] *« Comme je l'ai dit il y a quelques jours, la première mission de l'État, c'est bien de protéger nos concitoyens et d'assurer la sécurité du territoire. En effet, nous vivons dans un monde plein d'incertitudes où la nature de la menace a profondément changé et ce qui fait votre quotidien depuis maintenant plusieurs années a profondément évolué »,* URL : ttps://www.elysee.fr/emmanuel-macron/2017/10/18/discours-du-president-de-la-republique-emmanuel-macron-devant-les-forces-de-securite-interieure

[288] *« La proposition de loi vise à permettre précisément cela : savoir être inventif et innovant afin de renforcer le continuum de sécurité, tout en respectant pleinement les identités et les missions de chacun des acteurs qui y contribuent. Elle vise aussi à doter chacun d'entre eux des moyens et des ressources pour assurer plus efficacement et plus simplement les missions qui leur sont confiées »,* Proposition de loi n° 3452, *préc*, Exposé des motifs.

mémoire, l'article 4 du Règlement générale sur la protection des données personnelles[289].

83. Il convient à présent de s'intéresser, à l'article 24 qui « *prohibe l'usage malveillant de l'image des policiers nationaux et militaires de la gendarmerie en intervention* »[290], article le plus controversé de la proposition de loi dite « sécurité globale ».

En effet, après de nombreux débats politiques et médiatiques, ce texte a connu quelques modifications dont le contexte permet d'affirmer le lien existant entre les données personnelles et la notion d'ordre public, aussi, voici comment s'articulait sa première rédaction, « *I. – Le paragraphe 3 du chapitre IV de la loi du 29 juillet 1881 sur la liberté de la presse est complété par un article 35 quinquies ainsi rédigé : « Art. 35 quinquies. – Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait de diffuser, par quelque moyen que ce soit et quel qu'en soit le support, dans le but qu'il soit porté atteinte à son intégrité physique ou psychique, l'image du visage ou tout autre élément d'identification d'un fonctionnaire de la police nationale ou d'un militaire de la gendarmerie nationale lorsqu'il agit dans le cadre d'une opération de police. » II. – Les dispositions de l'article 35 quinquies de la loi du 28 juillet 1881 sur la liberté de la presse ne font pas obstacles à la communication, aux autorités administratives et judiciaires compétentes, dans le cadre des procédures qu'elles diligentent, d'images et éléments d'identification d'un fonctionnaire de la police nationale ou d'un militaire de la gendarmerie nationale* »[291].

Le contenu de cette proposition de loi, mais surtout de l'article précité, est pour l'opposition, amère et sans appel, il est contraire à la liberté d'information[292] et de

---

[289] RGPD art. 4, *préc*.

[290] Proposition de loi n° 3452, *préc*, Exposé des motifs.

[291] Art. 24, Proposition de loi n° 3452, *préc*.

[292] « *Cette proposition de loi soulève des risques considérables d'atteinte à plusieurs droits fondamentaux, notamment au droit à la vie privée et à la liberté d'information (…) particulièrement les restrictions envisagées concernant la diffusion d'images des agents des forces de sécurité dans l'exercice de leur fonction* »,
URL : https://defenseurdesdroits.fr/fr/communique-de-presse/2020/11/proposition-de-loi-securite-globale-lalerte-de-la-defenseure-des-droits

ce fait incompatible avec la liberté de la presse[293]. C'est pourquoi les acteurs de la presse et des médias ne sont pas restés de marbre énonçant certaines critiques à son égard, par exemple, par voie de communiqué adressé au Premier ministre, Jean Castex[294].

Pour la majorité en revanche, l'article 24 est une nécessité pour « *protéger ceux qui nous protègent* »[295], cette expression étant identique à ce que réclamait, déjà en 2016, Eric Ciotti, député LR des Alpes-Maritimes, suite à l'agression de policiers[296]. Conscient des différentes inquiétudes, à l'égard de la portée de ce texte, le gouvernement estime devoir « *clarifier les choses* »[297], mais martèle, néanmoins, qu'il ne s'agit « *évidemment pas d'une interdiction de filmer et de diffuser des policiers en manifestations ou en intervention* »[298], propos corroboré par le délégué général du syndicat Alliance police nationale qui accueille favorablement cette mesure[299].

Deux points de vue différents et divergents s'affrontent quant à la nécessité de la proposition de loi sécurité globale. Si l'opposition prétend que le texte en général et plus particulièrement l'article 24 contreviendrait à des principes démocratiques et fondamentaux tels que la liberté d'expression, la liberté d'informer ou bien

URL : https://www.lemonde.fr/societe/article/2020/11/04/loi-de-securite-globale-une-proposition-pour-limiter-la-captation-d-images-sur-le-terrain_6058525_3224.html

293 « *L'article 24 de la future loi ''sécurité globale'' menace la liberté d'informer* », URL : https://www.lemonde.fr/idees/article/2020/11/10/l-article-24-de-la-future-loi-securite-globale-menace-la-liberte-d-informer-alertent-des-societes-de-journalistes_6059188_3232.html

294 « *Depuis plusieurs semaines, nous constations avec inquiétude la multiplication d'initiatives législatives et politiques susceptibles d'attenter à la liberté de la presse. Celle-ci est pourtant le fondement de notre métier, mais surtout de toute vie démocratique* », URL : https://www.alliancepresse.fr/actualite/loi-sur-la-securite-globale/

295 URL : https://www.bfmtv.com/police-justice/il-faut-proteger-ceux-qui-nous-protegent-le-depute-sylvain-maillard-appelle-a-armer-la-police-municipale-parisienne_AV-202011170126.html

296 URL : https://www.lefigaro.fr/actualite-france/2016/10/11/01016-20161011ARTFIG00245-eric-ciotti-proteger-ceux-qui-nous-protegent.php

297 URL : https://www.francetvinfo.fr/replay-radio/8h30-fauvelle-dely/deconfinement-commerces-fermes-securite-globale-le-8h30-franceinfo-de-gabriel-attal_4170583.html

298 URL : https://twitter.com/i/status/1328594706599653386, URL : https://www.youtube.com/watch?v=uII6Ld4h8ik

299 « *Il n'y a aucune atteinte liberticide au droit et à la loi de la presse* », URL : https://www.francetvinfo.fr/faits-divers/police/proposition-de-loi-securite-globale-il-n-y-a-aucune-atteinte-liberticide-au-droit-et-a-la-loi-de-la-presse-assure-le-syndicat-alliance-police_4184543.html

même la liberté de la presse, la majorité se défend en arguant du fait que le besoin de sécurité ne recouvre en aucune manière une intention d'interdire ou même d'amoindrir certaines libertés[300].

Aussi, le recours à la notion d'ordre public semble être synonyme de dénouement pour cette situation délicate : grâce à cette dernière, un consensus pourrait être trouvé préservant, ainsi, les intérêts et considérations de chacun. Pour preuve, la nouvelle rédaction de l'article 24 démontre qu'une telle démarche est rendue possible. Désormais, ce texte sanctionne « *La provocation, dans le but manifeste qu'il soit porté atteinte à son intégrité physique ou psychique, à l'identification d'un agent de la police nationale, d'un agent des douanes lorsqu'il est en opération, d'un militaire de la gendarmerie ou d'un agent de la police municipale lorsque ces personnels agissent dans le cadre d'une opération de police* »[301], ce qui ne correspond plus à la diffusion d'images. Une telle modification permettant toujours de protéger les forces de l'ordre contre la volonté malveillante de les identifier à l'occasion des opérations de police, sans, toutefois, entraver de quelque manière la liberté de la presse[302].

Si la liberté d'expression, le droit à l'information des journalistes et la liberté de la presse relevant de la loi du 29 juillet 1881[303] doivent être évidements respectés, il n'en demeure pas moins que ces droits fondamentaux peuvent entrer en conflit et partiellement s'effacer devant d'autres lois ou principes. En l'espèce, lorsque cela est nécessaire, la liberté de la presse, dans sa globalité, doit s'éclipser, laissant place au respect de la vie privée. Le nouvel article 24 vient donc restaurer le

---

[300] « *Notre travail est de protéger les policiers et les gendarmes, très largement attaqués ces derniers temps (…) et en même temps de garantir, bien évidemment, la liberté d'informer. Les journalistes pourront toujours filmer, diffuser ces images. Pour résumer l'article 24 de la proposition de la loi sur la sécurité globale, filmer : oui, traquer les policiers : non* », URL : https://www.europe1.fr/emissions/linterview-politique-de-8h20/gerald-darmanin-assure-que-les-citoyens-pourront-toujours-filmer-les-operations-de-police-4006392

[301] C. pén., art. 226-4-1-1.

[302] « *La finalité est d'assurer une protection efficace des forces de l'ordre contre la volonté malveillante de les identifier à l'occasion des opérations de police tout en garantissant la liberté de la presse »,* C. Stoclin-Mille, *La Commission des lois du Sénat réécrit l'article 24 de la loi Sécurité globale*, Dalloz actualité, 5 mars 2021.

[303] Loi du 29 juillet 1881 sur la liberté de la presse.

respect dû à l'image des forces de l'ordre donc à leurs propres données personnelles puisque, est-ce nécessaire de le rappeler, l'image d'une personne est une composante, un fragment de sa personnalité, de sa vie intime et est à ce titre protégée.

Dans cette affaire, la référence à l'ordre public a permis un réel soutien aux données personnelles, sans contrevenir à l'intérêt général de la société, ni aux libertés fondamentales de celle-ci. Le nouvel article 24 de la proposition de loi « sécurité globale » n'exclut et n'interdit pas la captation d'images des forces de l'ordre, quelles qu'elles soient, lorsque ces dernières ne peuvent pas être reconnues[304]. Pour mémoire, les données strictement anonymes, ne sont pas des données personnelles et ne relèvent donc pas du champ d'application du règlement UE 2016/679.

La protection de la vie privée, principe d'ordre public énoncé par l'article 9 du Code civil[305], s'impose donc, avec dans son sillage le respect aux données personnelles dont l'image propre aux forces de l'ordre. Ainsi l'article 24 de la loi sécurité globale musèle toute provocation à l'identification de forces de l'ordre lorsque ces dernières sont valablement identifiées, évitant ainsi toutes formes de violence à leur égard[306].

84. Voilà en quoi la conformité des données personnelles et de leur utilisation à l'ordre public est importante en droit français. Encore une fois, l'idée majeure qui se dégage est celle d'une protection accrue des données personnelles, données sensibles et intimes. Le développement croissant d'internet et la multiplication des réseaux sociaux représentent, au quotidien, un danger pour les données personnelles, ce que les personnes concernées ont parfois du mal à percevoir. Il est donc pertinent de se féliciter de l'apport du règlement général sur la protection

---

304 « *Le but de l'article 24 ne consiste qu'à interdire la diffusion et non la captation d'images, dont le seul objectif serait de nuire à un fonctionnaire ou à un militaire de la gendarmerie, et d'attenter à sa sécurité physique ou psychique* », Le droit à l'information sur la justice, Questions – débats, Légipresse, 2021/HS1 (n° 65), p. 43-46.

305 C. civ., art. 9, *préc.*

306 « *Cet article a été rendu nécessaire par la diffusion de vidéos de force de l'ordre sur internet, qui pouvait entrainer menaces ou agressions contre le fonctionnaire concerné* », C. Stoclin-Mille, *La Commission des lois du Sénat réécrit l'article 24 de la loi Sécurité globale*, *Op cit*.

des données personnelles, ce dernier permettant aux personnes concernées par la collecte des données personnelles de l'importance de celles-ci.

En définitive, plus que de, simplement, constater la conformité des données personnelles et de leur utilisation à l'ordre public, il est possible, à présent, d'affirmer que l'ordre public est un soutien incontestable à la protection des données à caractère personnel, la double fonction de l'ordre public ainsi résumée à savoir que, « *l'ordre public et la protection des données personnelles, un mécanisme d'éviction et un instrument de hiérarchisation* »[307].

La pensée de l'auteur précité est approfondie et expliquée par une professeure laquelle estime, d'une part, que l'ordre public permet de guider ou d'écarter certaines pratiques contractuelles et, d'autre part, qu'il est un moyen utilisé pour recentrer des valeurs fondamentales[308].

En effet, dans un premier temps, l'ordre public, norme supérieure, impose dans le cadre de la protection des données personnelles un contenu contractuel obligatoire et ce, tout d'abord, dans la relation entre le responsable de traitement et le sous-traitant, mais aussi, concernant le phénomène des transferts de données hors de l'Union européenne. Si les contrats présentés se voient régis et figés par un ordre public contractuel[309], il arrive, à l'inverse, que lorsque certains contrats se heurtent à celui-ci, l'ordre public contribue à écarter et donc invalider ces derniers pour non-respect de la norme supérieure.

85. Mécanisme d'éviction, l'ordre public se révèle être, dans un second temps, un instrument de hiérarchisation pour la protection des données personnelles, laquelle entretient un lien étroit avec le respect de la vie privée[310]. Pour ce faire, il s'implique dans l'arbitrage de la relation et l'articulation entre la libre circulation de l'information sur internet et le respect des libertés fondamentales

---

307 M. Mekki, *L'intérêt général et le contrat, Contribution à une étude de la hiérarchie des intérêts en droit privé,* LGDJ, 2004, n° 292.

308 A. Danis-Fatôme, *Ordre public et protection des données à caractère personnel*, *Op cit*, p. 366.

309 *« L'ordre public est le cadre normal de la liberté contractuelle »*, J. Ghestin, *L'ordre public, notion à contenu variable, en droit privé français*, *préc*, p. 83.

310 « *On comprend que l'ordre public soit en jeu lorsqu'on s'intéresse à la protection des données personnelles car celle du respect de la vie privée est sous-jacente* », M.-P. Fennol-Trousseau et G. Haas, *Internet et protection des données personnelles*, Litec, 2000, p. 1.

des personnes[311]. Le second rôle attribué à l'ordre public s'apprécie à travers l'éclosion du consentement en matière de données personnelles,[312] lequel sera, pour le bien des personnes concernées, soumis par cet instrument de hiérarchisation[313].

Si la notion d'ordre public, principe essentiel de l'ordre juridique français, semblait pour le moins difficilement perceptible, il n'en demeure pas moins qu'elle se révèle être un allié, non négligeable, pour les données personnelles.

Il n'est pas nécessaire de s'émouvoir, par le Règlement général sur la protection des données personnelles, qui se veut « chevalier défenseur » des personnes, l'utilisation des « données personnelles » de ces derniers ne semble pas pouvoir outrepasser le cadre de l'ordre public.

86. Les dérives qui pourraient exister, dans un futur (qu'il faut espérer le plus lointain), telles que la question du clonage, du transgénisme ou toutes autres manipulations génétiques humaines, ne semblent pas encore être d'actualité.

Pour synthétiser, la mise en place du Règlement européen, en ce qu'il impose aux responsables de traitement de ne rassembler que les informations nécessaires et de s'assurer du consentement éclairé des intéressés, se présente comme un véritable bouclier contre la transgression de l'utilisation des « données personnelles » à l'ordre public.

87. Toutes ces craintes ont, pourtant, aussi vocation à exister quant à l'utilisation des « données personnelles » et le respect aux bonnes mœurs.

---

311 M.-P. Fennol-Trousseau et G. Haas, *Internet et protection des données personnelles*, *Ibid*, p. 1.

312 *« Le rôle important du consentement de la personne concernée dans le droit de la protection des données personnelles pose la question du recul de l'État dans un dispositif qui vise à garantir les droits fondamentaux »*, J. Le Clainche et D. Le Métayer, *Données personnelles, vie privée et non-discrimination : des protections complémentaires, une convergence nécessaire*, RLDI févr. 2013, p. 80 s., spéc. p. 91.

313 *« Le consentement de la personne concernée ne sera jamais dans le droit de la protection des données personnelles une forme de blanc-seing qui permettrait à un responsable de traitement de s'affranchir des règles conditionnant la licéité d'un traitement »*, A. Debet, J. Massot et N. Metallinos, *Informatiques et Libertés*, Lextenso éditions, 2015.

§2 La conformité des données personnelles aux bonnes mœurs

88. Dans l'objectif de rapprocher les « données personnelles » aux bonnes mœurs et dans l'intention de confronter ces deux concepts, il convient naturellement d'explorer la notion de « bonne mœurs », la notion relative aux « données personnelles » étant, quant à elle, déjà développée à maintes reprises.

89. En amont de cette opération, consistant à rapprocher les données personnelles aux bonnes mœurs, il apparait, premièrement, judicieux, pour ne pas les confondre, d'écarter et de dissocier les notions de bonnes mœurs et d'ordre public. En effet, le concept d'ordre public, approfondi préalablement, et celui de bonnes mœurs apparaissaient si proches, si voisins, qu'il n'est pas rare, ni anodin, de vouloir les confondre. Au milieu du XX^{e} siècle, Marty et Raynaud précisent, déjà en ce sens, que « *la notion de bonnes mœurs est bien proche de celle d'ordre public* »[314], là où plus encore, en précisant que « *Historiquement, l'ordre public a pris sa source dans les bonnes mœurs* »[315], un autre auteur affirme la proximité de ces deux notions et rappelle ainsi leur influence mutuelle.

Si de nos jours, l'ordre public est souvent déclaré comme l'antithèse à la liberté contractuelle, c'est-à-dire une barrière à l'autonomie de la volonté individuelle, cette notion recouvre une réalité, dont la finalité s'inspire du concept de bonnes mœurs. Si dans l'histoire, la notion de bonnes mœurs permettait de protéger la société en posant certaines limites à ne pas franchir, lorsque certaines considérations ont semblé désuètes car trop individualistes, le recours à cet impératif s'est peu à peu essoufflé laissant place à l'ordre public. Voilà pourquoi, le lien entre ces deux principes est indéfectible, les bonnes mœurs semblent être un modèle, sinon une aspiration pour l'ordre public, ce dernier ayant plus de facilité pour s'adapter à l'évolution de la société, notamment parce que cette notion s'apprécie dans un sens plus large et permet de répondre à davantage de nouvelles problématiques.

---

[314] G. Marty et P. Raynaud, *Traité de droit civil, Les obligations t. 1*, Les sources, 1988, Sirey, n°77.

[315] M. Pena, *Les origines historiques de l'article 6 du Code civil* dans R.R.J., P.U.A.M., n° XVII-49, 1992-2.

Si grammaticalement ces termes ne se ressemblent, en aucun point, cela prouve qu'ils sont loin d'être synonymes et qu'ils peuvent donc exister à part entière. Ces notions s'épanouissent donc séparément et ont vocation à subsister, à survivre, peut-être différemment, chacun de leur côté.

Alors qu'à l'origine, « *leurs fonctions sont identiques* »[316], dans le sens où « *comme l'ordre public, le respect des bonnes mœurs contribue au maintien de l'ordre social et à la préservation d'une certaine conception de l'intérêt général* »[317], l'approche moderne de celles-ci consiste, peu à peu, à les éloigner, non pas de manière stricte et définitive, mais au moins sur certains points.

Il s'avère, aujourd'hui, possible d'énoncer que l'ordre public semble être une notion éminemment plus utilisée sans pour autant affirmer que le recours aux bonnes mœurs n'existe plus, il est cependant plus en retrait. En effet, l'ordre public est une notion qui ne cesse d'être pratiquée au sein du monde juridique et reste surtout plus respectée par les individus et la société en général, peut-être car mieux comprise, mieux appréhendée, donc plus crainte.

Les différents changements de société conduisent à certaines évolutions quant à l'approche de ces notions. Si d'un côté, l'ordre public parait, naturellement, s'imposer à la société tout entière, de l'autre, c'est la société qui, de son bon vouloir, semble se référer, ou non, à la notion de bonnes mœurs.

Voici que la question de la perception est, peut-être, l'une des différences les plus ostensibles entre ces notions, elles qui ont pourtant des ambitions et fonctions communes. Pour le dire plus simplement, la référence aux bonnes mœurs se rapproche du symbole et du mystique en étant supérieure aux individus et à la société, tandis que la référence à l'ordre public représente une idée cartésienne, ancrée, comme confondue avec l'intérêt général.

---

316 G. Marty et P. Raynaud, *Traité de droit civil, Les obligations t. 1*, *Op cit*, n°77.

317 J-J. Lemoulad, G. Piette, J. Hauser, *Ordre public et bonnes mœurs*, Ed. Dalloz, RDC Février 2019 (actualisation Décembre 2019).

Si la notion de bonnes mœurs, qui a principalement vocation à s'intéresser et à venir en aide à l'individu, parait avoir une connotation aussi spirituelle, c'est à cause de son rapport à la morale. En effet, ce concept est fortement inspiré par la religion (exemple avec le délit d'adultère), elle qui tient une place importante dans l'histoire française, mais également par la philosophie (exemple avec le non-respect de la dignité de la personne).

Quant à l'ordre public, cette notion semble destinée à sauvegarder et protéger l'intérêt général, en témoigne son utilisation, dès le XIX[e], comme unique moyen permettant tranquillité et salubrité publique[318]. Plus récemment, le renforcement de la préservation de l'ordre public comme principal objectif du projet de loi confortant le respect des principes de la République démontre sa vocation[319], celle de subvenir aux besoins d'un ensemble plus qu'à un seul individu.

Cette dichotomie est également directement remarquée quant à la notion de bonnes mœurs, « *Dans une conception empirique, les bonnes mœurs englobent l'opinion de la masse et ses comportements habituels. A l'inverse, dans une conception idéaliste, elles s'apparentent à une sorte d'éthique supérieure, naturelle ou divine* »[320].

Les complémentarités et différences entre ces notions étant dévoilées, il est désormais temps de recentrer l'étude en question sur la conformité des données personnelles aux bonnes mœurs. Pour ce faire, il s'agit d'abord de définir les bonnes mœurs, puis d'en démontrer l'interaction avec les données à caractère personnel.

90. Si anciennement les bonnes mœurs permettaient d'identifier « l'honnête homme » en ce qu'elles étaient « l*es règles de morale sociale considérées comme fondamentales pour l'ordre même de la société* »[321], à l'époque actuelle, la notion ne s'entend plus exactement de la même façon.

---

[318] Ordre public (Droit administratif), Fiche d'orientation, Dalloz, Septembre 2020, URL : https://www-dalloz-fr.ezproxy.univ-perp.fr/documentation/Document?id=DZ/OASIS/000687

[319] C. Stoclin-Mille, *La préservation de l'ordre public dans le projet de loi confortant le respect des principes de la République*, Dalloz actualité, 17 février 2021.

[320] J-J. Lemoulad, G. Piette, J. Hauser, *Ordre public et bonnes mœurs*, *Op cit*.

[321] F. Terré, Ph. Simler, Y. Lequette, *Droit civil : les obligations*, *Op cit*, p. 433.

Avec la réforme du droit des obligations, la disparition de l'article 1133 du Code civil en ce qu'il disposait anciennement que « *La cause est illicite quand elle est prohibée par la loi, quand elle est contraire aux bonnes mœurs ou à l'ordre public* »[322] et par là, la disparition de la « cause » permet d'établir que la dimension même des bonnes mœurs a changé.

Pour trouver une survivance de ce concept dans le Code civil, il faut désormais s'intéresser à l'article 6 qui prétend que « *On ne peut déroger, par des conventions particulières, aux lois qui intéressent l'ordre public et les bonnes mœurs* »[323]. C'est à remarquer, l'Ordonnance portant réforme du droit des obligations a conservé la référence à cette notion. Un tel maintien s'explique d'une part à travers une logique et un réflexe conservateur, à savoir une volonté pour le législateur de maintenir les bonnes mœurs contractuelles en droit moderne afin d'éviter tout relâchement par certaines pratiques, d'autre part cela prouve que le concept de bonnes mœurs peut évoluer et s'adapter, sa fonction n'étant plus seulement d'ordre sexuel mais s'attachant aujourd'hui à bien d'autres considérations, faisant croire pour certains auteurs à l'émergence d'une « nouvelle moralité publique ».

De nos jours, si la notion de bonnes mœurs ne repose plus seulement dans une dimension sexuelle ou morale, elle reste quand même une forme d'éthique du contrat au regard notamment de la bonne foi contractuelle et de toutes situations d'abus. Un tel constat, réalisé après la réforme du droit des obligations et de la preuve, énonçant la survivance et l'importance des bonnes mœurs par rapport au droit des contrats, était, déjà, celui dressé quelques années auparavant, comme en atteste la pensée de Louis-Frédéric Pignarre, lui qui avait ces propos « *Autant le discours sur les bonnes mœurs s'est effacé en droit des personnes et de la famille, autant il est prégnant en droit des contrats* »[324].

---

[322] C. civ., anc. art. 1133 *(Abrogé par Ord. n° 2016-131 du 10 févr. 2016, à compter du 1er oct. 2016)*.

[323] C. civ., art. 6, *préc.*

[324] L-F. Pignarre, *Que reste-t-il des bonnes mœurs en droit des contrats ? « Presque rien ou presque tout ? »*, RDC 2005. 1284.

91. Visionnaire, la notion de bonne mœurs semble suivre les évolutions sociétales et peut, dès aujourd'hui, parfaitement coller avec la question des « données personnelles ».

Déjà en 1913, la Cour d'appel de Lyon, par un arrêt rendu le 27 juin semblait, étonnamment, se rapprocher de cette question, les magistrats estimant au sujet d'expérimentation corporelle que « *Toute convention visant à réaliser des expériences sur le corps humain est nulle comme contraire à l'ordre public et aux bonnes mœurs dès lors que l'opération ne présente aucun intérêt pour le patient* »[325].

La mise en place du Règlement général sur la protection des données et la prise de conscience autour de la protection des « données personnelles » est naturellement à rapprocher de l'idée véhiculée par la notion de bonnes mœurs, d'autant plus, comme cela a été dit, la dimension de ce concept a évolué.

92. Plusieurs interrogations se développent donc, par exemple, est-il normal que certaines conventions, portant sur les « données personnelles » font subir pression et dépendance économique, alors que cela est totalement contraire à ce qui ressort de l'exigence des bonnes mœurs ?

Il ne faut pas se mentir, les « données personnelles » sont des données rares, sensibles, et riches en information et pour ces raisons, il n'est pas impossible que des contractants malveillants abusent de leur position pour soutirer ce genre d'informations.

L'abus de position économique ou l'abus de position dominante peuvent permettre « d'imager » les propos précédents. En effet, que reprocher à un utilisateur ordinaire, et peut-être un peu naïf, qui se confronterait aux géants des réseaux sociaux tels que Facebook, Google ou Instagram et qui, par ce que ces derniers abusent de leurs statuts, se ferait soutirer des informations. Il est question ici d'individus qui se rendent sur des réseaux sociaux et qui partagent leur vie

[325] CA., Lyon, 27 juin 1913.

privée, en toute confiance. Le fait d'être derrière un écran ou de poster sur internet des fragments de sa vie privée désacralise l'intimité de chacun. Les individus, qui dans la vie de tous les jours ont pleinement conscience de l'intérêt de protéger leur vie privée, adoptent sur internet un comportement bien différent et s'exposent beaucoup plus facilement. Ce constat alarmant est celui partagé par un spécialiste des stratégies numériques qui résumé ces manœuvres par ce qu'il nomme être un paradoxe de l'intimité[326].

Le paradoxe précité n'existe, malheureusement, que parce les « GAFA[327] » ou plus récemment « GAFAM[328] » existent. Si les biens faits de ces firmes ne sont plus à prouver, le monde entier peut, en effet, au quotidien bénéficier de ces multiples évolutions techniques, technologiques et sociétales, pour autant quelques zones d'ombres, non négligeables, pour les utilisateurs sont à souligner. Tel « le revers de la médaille », le prix à payer pour se servir et jouir de ces plateformes est l'abandon de sa liberté, de sa vie privée, par la transmission de ses propres données personnelles et cela en y consentant ou non !

L'étude de la conformité des données personnelles aux bonnes mœurs a donc vocation à se poursuivre avec comme étendard les controverses engendrées par les géants du web dit « GAFA », utilisant à mauvais escient leur position dominante. C'est par l'utilisation malhonnête des données personnelles par ces firmes que le non-respect aux bonnes mœurs est le plus flagrant.
Déjà en 2013, avant l'instauration du nouveau règlement en faveur de la protection des données personnelles, certaines associations de consommateurs déploraient et critiquaient les conditions d'utilisation des géants du web[329], eux

---

326 *« Les utilisateurs, conscients théoriquement de l'importance de protéger leur vie privée ont en réalité un comportement généralement opportuniste et négligeant dans leur exercice intime des plateformes digitales. C'est le fameux ''paradoxe de l'intimité'' »,* URL : https://www.marianne.net/agora/humeurs/face-aux-gafa-nos-donnees-sont-notre-liberte

327 Acronyme utilisé pour désigner les quatre géants du web, à savoir : Google, Apple, Facebook et Amazon.

328 Acronyme utilisé pour désigner les cinq géants du web, la firme Microsoft étant rajoutée.

329 *« Les contrats d'utilisation sont très opaques, inaccessibles, incompréhensibles pour les internautes, ils sont même parfois en anglais. C'est dire si, tout ce que s'autorise à faire le réseau social, n'est pas avec un consentement exprès de l'utilisateur »,* A. Bazot, Président directeur de l'UFC-Que Choisir, Source : FR 3 – 19/20, Edition nationale, Journal télévisé, 27 juin 2013.

qui usaient de leur position pour entraver la confidentialité des données des internautes, des utilisateurs de réseaux sociaux ou de moteur de recherche[330].

Si les bonnes mœurs représentent « *ce qui est moral »*[331]*,* l'attitude des « GAFA », consistant à utiliser une position dominante pour alimenter un commerce juridique des données personnelles, sans l'avis des principales concernées, c'est-à-dire les personnes dont les données sont collectées, utilisées et revendues, est une démarche, pour le moins, choquante et immorale. Ainsi était la situation avant l'entrée du RGPD, aussi quid de l'impact du Règlement aujourd'hui ? Les firmes dites « GAFA » se sont-elles soumises, conformées, au principe de bonnes mœurs sous l'impulsion dudit règlement ? De nombreux et récents scandales, permettent, malheureusement, de répondre à l'interrogation soulevée en amont. Pour résumer la situation, les dérives des « GAFA » n'ont pas été anéanties par l'entrée en vigueur du nouveau règlement. Pour autant, il ne faut pas tirer de conclusion trop hâtive et n'y voir qu'un échec, une prise de conscience croissante est en marche et doit continuer à se poursuivre.

93. Quoi de mieux pour illustrer les propos, précédemment, avancées que de se concentrer sur l'une des plus grandes crises du réseau social « Facebook », l'affaire « Cambridge Analytica ».

Cette société spécialisée dans les technologies de l'information et de la communication est mondialement connue car elle accusée d'avoir organisé la collecte des données personnelles de millions d'utilisateurs du réseau social Facebook dans le monde[332]. Les dessous de l'affaire « Cambridge Analytica »

---

330 « *On peut regarder le contenu de vos mails, le contenu des documents que vous avez mis sur Google-docs et combiner toutes ces informations pour offrir des publicités personnalisées, pour offrir de nouveaux services* », G. Le Grand, secrétaire adjoint de la CNIL, Source : FR 3 – 19/20, Edition nationale, Journal télévisé, 27 juin 2013.

331 « *Notions imprécises et relatives par excellence, les notions de bonne moralité et de bonnes mœurs renvoient à ce qui est moral, au « respect des idées morales communément admises à un moment donné par la moyenne des citoyens »*, Conclusions du commissaire du Gouvernement sur CE, sect. 20 déc. 1957, Sté nationale d'éditions cinématographiques, *Lebon*702.net

332 *« Au total, nous pensons que les informations concernant jusqu'à 87 millions de personnes – principalement aux États-Unis – ont pu être partagé à tort avec Cambridge Analytica »,* URL : https://www.lemonde.fr/pixels/article/2018/04/04/cambridge-analytica-87-millions-de-comptes-facebook-concernes_5280752_4408996.html

révèle, en réalité, que la firme londonienne achetait les données personnelles d'utilisateurs connectées sur l'application « ThisIsYourDigitalLife »[333].

Pour comprendre comment une telle opération peut exister, il faut bien avoir à l'esprit que le commerce de données personnelles représente une partie du cœur du modèle économique des GAFA[334]. Une telle marchandisation des données personnelles ne peut reposer, sur une base saine, c'est-à-dire une base qui serait imprégnait d'une croyance et d'une conformité aux bonnes mœurs, le concept de marchandisation en étant aux antipodes. Ce bilan, alarmant, est celui dégagé par le lanceur d'alerte à l'origine du scandale précité, qui dénonce la malhonnêteté qui anime les « GAFA », pour ce dernier ces manœuvres n'ont rien d'étonnant, « *Les produits Facebook sont conçus par des ingénieurs, des designers-produit, des data scientist. Or, à l'inverse de leurs collègues d'autres secteurs, comme l'aéronautique ou la construction, ces derniers n'ont aucun cadre éthique auquel se référer* »[335].

94. Si, depuis 2013, l'intention malveillante qui anime les grandes puissances du numérique n'a pas eu vocation à s'arrêter de manière définitive, cette démarche tend pour autant à s'estomper peu à peu, notamment par une forme de méfiance et de prise de conscience des personnes concernées par les collectes, demeurant, inconsciemment, ainsi l'une des plus grandes avancées du Règlement européen[336].

---

333 *« Son principe est simple, elle propose de payer des utilisateurs pour remplir des tests psychologiques en accédant à leurs données sur Facebook. Sauf qu'en réalité, Aleksandr Kogan revend ces données à Cambridge Analytica »,* URL : https://siecledigital.fr/2018/03/23/cambridge-analytica-tout-comprendre-sur-la-plus-grande-crise-de-lhistoire-de-facebook/

334 *« Pour ces leaders de l'économie numérique, ces données personnelles sont le carburant qui les fait avancer. Une donnée personnelle isolée, par exemple, un numéro de téléphone rattaché à un nom vaut tout au plus quelques centimes, mais une fois agrégé avec d'autre informations, elle dresse un profil complet de chaque internaute que les GAFA savent monétiser à merveille. Facebook tire de cette marchandisation des données personnelles 98% de ses 40 milliards de dollars de revenu annuel en 2017 »,* URL : https://christian-buhlmann.com/pourquoi-les-gafa-sinteressent-ils-tant-a-vos-donnees-personnelles/

335 URL : https://www.ladn.eu/tech-a-suivre/christopher-wylie-cambridge-analytica-menaces-democraties/

336 *« 71% des personnes interrogées s'inquiètent de la façon dont les géants de la technologie recueillent et utilisent leurs données personnelles. Sept personnes sur 10 veulent que les gouvernements règlementent les activités des géants de la technologie en raison d'inquiétudes quant aux données personnelles »,* URL : https://www.amnesty.fr/liberte-d-expression/actualites/gafa-gestion-des-donnees-personnelles

Pour rebondir sur l'inquiétude des individus et l'aide demandée aux gouvernements, il semble qu'une réelle avancée est de mise à ce sujet. En effet, le 1er décembre 2020, Emmanuel Macron, « *s'est félicité de la signature d'un appel par 75 acteurs du numérique, le ''TechForGood*[337]*''* »[338], initiative lancée par le Président de la République française, convaincue que si la technologie est synonyme de progrès majeurs, elle comporte notamment quelques revers lorsque des acteurs s'éloignent des valeurs originelles du Web[339].

95. Si les bonnes mœurs sont une référence moins importante que ne l'est, par exemple l'ordre public, pour les données personnelles, il n'en demeure pas moins qu'en raison de certaines dérives, ce principe soit toujours important. Les bonnes mœurs recouvrent une certaine éthique, une certaine moral, un comportement décent à avoir en présence de données si sensibles et privées que sont les données personnelles. En somme les bonnes mœurs font appel à la bonne foi contractuelle pour tous les acteurs qui collectent et usent des données, et qui en profitent, parfois, pour en abuser. Ces dérives sont le fruit de position dominante de la part des grandes firmes du numérique, dit « GAFA », qui n'hésitent pas à outrepasser la vie privée de leurs utilisateurs à des fins commerciales.

96. Heureusement, le Règlement général sur la protection des données personnelles, à l'aune de certains grands principes, est attentif, notamment en veillant de garantir la conformité de l'utilisation des « données personnelles » aux bonnes mœurs, notion ancienne, mais toujours d'actualité. Si le concept de bonnes mœurs semble, actuellement, en retrait, passé de mode, notamment du fait de son caractère symbolique ou spirituel, en rapport avec la morale ou l'éthique, il reste tout de même une référence sur lequel se reporter, ce qui est le cas par exemple pour les données personnelles, puisque les bonnes mœurs représentent la situation dans laquelle agirait un « honnête homme ». Malgré la suppression de l'ancien

---

337 URL : https://ww.elysee.fr/admin/upload/default/0001/09/9cbaf53e3475d20381db6c0959e00e19d72aa.pdf

338 URL : https://www.rtl.fr/actu/politique/les-gafa-s-engagent-a-etre-plus-vertueux-une-victoire-pour-macron-7800932946

339 *« Tous reconnaissent, en signant ce manifeste, leur impact, social, sociétal et environnemental »,* URL : https://www.elysee.fr/emmanuel-macron/2020/12/01/tech-for-good-plus-de-75-leaders-sengagent

article 1133 du Code civil, la notion de bonnes mœurs, qui perdure au sein de l'article 6 du Code civil, s'avère visionnaire de par sa capacité à s'adapter aux évolutions de la société. Concrètement, tout comme la notion d'ordre public, celle de bonnes mœurs apporte sa pierre à l'édifice et s'érige en rempart contre l'utilisation malhonnête des données personnelles, ce qui est par exemple le cas de la marchandisation des données par les géants de l'internet.

CONCLUSION DU CHAPITRE 2

Notion particulière, la donnée personnelle doit, pour s'épanouir en tant que fondement du but contractuel, se plier aux exigences de droit commun.

Si la donnée personnelle doit respecter l'impératif de licéité, cher au droit des contrats, l'utilisation de celle-ci doit également se conformer à l'ordre public et aux bonnes moeurs.

CONCLUSION DU TITRE 1

97. La donnée personnelle est un élément si particulier qu'elle obéit à un régime juridique particulier qui n'empêche pas, pour autant de relever du contenu contractuel. En effet, la donnée personnelle est tantôt un élément principal, tantôt, un élément secondaire à ce dernier.

98. Il n'en reste pas moins que la donnée personnelle est un élément fondateur du but contractuel qui se plie tant aux exigences de licéité de celui-ci, qu'à la conformité souhaitée par l'ensemble du droit commun.

TITRE 2

Le consentement au contrat au prisme des données personnelles

100. Si tous les éléments invoqués dans le premier Titre, à savoir les « données personnelles » en tant qu'élément relevant du contrat, se trouvent réunis, il est alors possible de contracter sur les « données personnelles » (Chapitre 1). Toutefois, il faut distinguer, spécialement au prisme du règlement général sur la protection des données, d'une part le consentement au contrat et d'autre part le consentement à l'utilisation de la donnée personnelle qui peut exister hors du champ du contrat (Chapitre 2).

Chapitre 1 : Le consentement au contrat portant sur les données personnelles

101. Le consentement devant être donné au contrat portant sur les données personnelles est d'abord et avant tout un consentement donné à un contrat, lui-même, portant sur les données personnelles, c'est-à-dire, en ce qu'elles en sont l'élément principal (Section 1). Pour autant, cette information ne doit pas masquer le fait qu'il existe des contrats dont les données ne sont qu'accessoires vis à vis d'une prestation dont celle-ci peut dépendre (Section 2).

Section 1 : Les contrats portant sur les données personnelles elles-mêmes

102. Afin de déterminer ce que sont les contrats portant sur les données personnelles et le rapport qu'ils entretiennent avec le consentement des parties, il convient de s'interroger sur la notion de consentement (Paragraphe 1), pour en déduire l'obligation d'information spécifique qui en résulte (Paragraphe 2).

§1 Qu'est-ce que le consentement ?

103. Si dans le langage commun le consentement est l'action d'accepter, d'acquiescer, de donner son accord à une action, un projet, une simple idée ou encore à une discussion entre amis[340], il faut avoir à l'esprit qu'en langage juridique le consentement se traduit différemment et se renforce, tant la portée de l'acte en question est singulière.

En effet, il est tout à fait logique que le consentement rencontré en droit des contrats présente certains critères, qui lui sont propres, et qu'il convient, cumulativement, de respecter, notamment du fait des conséquences en matière de responsabilité, ce qui permet de conforter ce dernier et de le différencier de celui présent dans la vie courante.

104. Afin de comprendre l'importance du consentement, au prisme du droit et plus particulièrement au droit des contrats, il convient, tout d'abord, d'apprécier celui-ci à travers l'histoire et notamment de le découvrir par le biais d'une brève approche originelle et philosophique.

---

[340] « *Provenant du latin cum-sentire (sentir avec), la notion de consentement désigne un accord, une conformité ou une uniformité d'opinion. Comme la permission ou l'agrément, le consentement est lité à des actions de la vie quotidienne ou l'événement dépend en partie de nous, en partie de la volonté des autres.* », P. Merlier, *Philosophie et éthique en travail social,* Politiques et interventions sociales, Presses de l'EHESP, 2013, p. 55-61.

Les prémices de la notion de consentement se retrouvent, dès l'Antiquité, grâce au mouvement philosophique du stoïcisme[341] qui lui attribue une première définition[342]. D'après ce courant philosophique, le consentement renverrait à une idée extérieure, qui s'imposerait à l'être humain, mais que ce dernier finirait par véritablement cautionner.

Une approche contemporaine associe le consentement, ce concept de philosophie morale, avec différentes conceptions que les philosophes se font de l'autorité. Trois exemples, parlants, permettent de saisir cette pensée moderne.

Selon l'inspiration de la sociologie durkheimienne, « *Très tôt, la société nous apprend à ne pas résister. A nous soumettre aux normes qu'elle nous impose* »[343], ce qu'Émile Durkheim énonçait, déjà, par ces mots « *Par autorité, il faut entendre l'ascendant qu'exerce sur nous toute puissance morale que nous reconnaissons comme supérieure à nous* »[344].

Pour d'autres penseurs, si le recours à la force physique permettait, autrefois, d'assouvir et d'imposer son autorité, depuis la révolution industrielle, intervenue au XIXe siècle, le consentement et les rapports d'autorité sont désormais sous des rapports de force politique[345].

En revanche, d'après le sociologue français Pierre Bourdieu, l'autorité s'impose lorsqu'elle est acceptée[346].

---

341 « *Le stoïcisme, courant philosophique grec et romain, se présente comme une doctrine panthéiste et matérialiste. Né au IVe siècle avant JC avec Zénon de Citium, le stoïcisme se développa jusqu'à la fin du IIIe siècle après JC* », URL : https://la-philosophie.com/le-stoicisme

342 « *Acte d'acceptation dirigé à l'endroit de quelque chose qui nous dépasse, contre quoi on ne peut rien, mais que l'on fait paradoxalement sien en acquiesçant à sa présence* », L. Monteils-Lang, *Perspectives antiques sur la philosophie du consentement*, Tracés. Revue de Sciences humaines [En ligne], n°14, 2008, p. 31-43.

343 S. Jankélévitch, *Du consentement à l'assujettissement*, dans G. Cahen (dir.), *Résister : le prix du refus*, Paris, Autrement, p. 124-138.

344 E. Durkheim, *L'éducation morale*, Paris : Librairie Félix Alcan, 1934.

345 « *Plutôt que de critiquer directement leurs employés, les patrons modernes préfèrent susciter des émotions fortes comme la honte ou le respect, afin de faire naitre un réflexe d'obéissance* », R. Sennett, *Autorité*, Paris : Fayard, 1982.

346 « *L'autorité ne s'impose pas toujours contre le gré des sujets qu'elle veut soumettre car les paroles émanant de l'autorité n'ont un sens que dans la mesure où ils sont délibérément reconnus par ceux qui s'y soumettent. L'autorité représenterait donc plus à un dialogue qu'à un simple monologue* », P. Bourdieu, *Ce que parler veut dire. L'économie des échanges linguistiques*, Paris, Fayard, 1982, p. 105.

Ces différentes idéologies exposent chacune, à leur manière, le fait que l'action dite du consentement s'imposerait naturellement aux personnes, pour diverses raisons, surtout d'autorité. Qu'elles soient de nature morale, politique ou encore symbolique, les individus n'auraient nul autre choix que d'y adhérer et donc de l'accepter, si tant est que l'autorité en question soit comprise et donc implicitement admise.

105. La notion de consentement venant d'être détaillée à l'aune d'un point de vue philosophique, il convient désormais de s'intéresser à celle-ci envers une approche toujours historique mais cette fois conjuguée, également, par une acception juridique. C'est en effet à l'avènement du consensualisme, en droit romain, qu'il faut, à présent, s'attarder.

Le développement à venir prend racine par l'allocution latine « *Solus consensus obligat* »[347], exprimant et résumant l'idée du consensualisme. Cette formule caractérise, à elle seule, le consensualisme, c'est-à-dire ce principe juridique qui est l'essence même de l'idée du consentement. Selon ce mécanisme, qui s'oppose à celui du formalisme, la conclusion d'une volonté commune des parties, un accord, suffit pour créer l'existence d'un contrat.

Né en droit romain, au service de quatre contrats qualifiés de « souples »[348], le consensualisme s'impose, en ce temps, du fait de l'évolution de la société, des échanges commerciaux et des relations juridiques de plus en plus répandues entre citoyens romains et non-romains[349]. Si le consensualisme est une évidence permettant la simplification des échanges et du commerce, il n'en demeure pas moins que certaines défaillances sont à déplorer. Voilà pourquoi, le dogme du formalisme, pourtant mentionné, comme une, vive, opposition au principe du consensualisme, s'immisce au soutien de ce dernier et cela principalement pour deux raisons, qui sont d'ailleurs toujours d'actualité.

---

[347] « Le consentement oblige à lui seul ».

[348] La vente, le louage, la société et le mandat.

[349] E. Charpentier, *Le rôle de la bonne foi dans l'élaboration de la théorie du contrat,* RDUS (Revue de Droit de l'Université de Sherbrooke), vol., 26, n°2, 1996, p. 306.

Si la première remarque, qui explique l'assistance du formalisme au consensualisme, concerne la complexité prolifère des contrats, la seconde explication de l'entraide entre ces deux notions, pourtant antonyme, est symbolisée par le souhait d'éviter, mais surtout de renforcer les engagements de consentements, trop souvent, pris avec légèreté.

106. Pour autant historique, puisque développé en droit romain, le consensualisme, qui a pu souffrir de la concurrence du formalisme, n'en reste pas moins actuel[350] et se retrouve désormais consacré à l'article 1109 nouveau alinéa 1er du Code civil qui dispose ainsi que « *Le contrat est consensuel lorsqu'il se forme par le seul échange des consentements quel qu'en soit le mode d'expression* »[351].

Voilà en quoi ce principe est, bien entendu, toujours évoqué, ce qui est, notamment, le cas à propos du contrat de vente[352]tel que le démontre la décision rendue le 12 novembre2015 par la 3e chambre civile de Cour de cassation, au visa, affirmé, de l'article 1583 du Code civil qui expose que la vente est « *parfaite entre les parties, et la propriété est acquise de droit à l'acheteur à l'égard du vendeur, dès qu'on est convenu de la chose et du prix, quoique la chose n'ait pas encore été livrée ni le prix payé* »[353] et celui, plus implicite, de l'adage latin « *Solus consensus obligat* ».

Il est question, en l'espèce, de la vente d'un immeuble d'une personne laquelle avait mandaté, pour ce faire, une société immobilière. Alors qu'un acquéreur semble intéressé et formule une contre-offre d'un certain montant, légèrement plus bas que l'estimation initiale, le propriétaire accepte celle-ci et l'acquiesce notamment par le biais de la formule « bon pour accord ». Mais voici que peu de temps avant de passer la vente, le propriétaire vendeur se rétracte.

---

350 M. Latina, *Contrat : généralité, éd. Dalloz, RTD. civ. 2017 (actualisation 2020)*.

351 C. civ., art. 1109 *(Ord. no 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

352 « *La vente est une convention par laquelle l'un s'oblige à livrer une chose, et l'autre à la payer. Elle peut être faite par acte authentique ou sous seing privé* », C. civ., art. 1582 (*Loi 1804-03-06 promulguée le 16 mars 1804*).

353 C. civ., art. 1583 (*Loi 1804-03-06 promulguée le 16 mars 1804*).

L'agence immobilière, ayant joué le rôle d'intermédiaire, entre l'acheteur et le vendeur, assigne ce dernier pour le versement d'une commission relatif à cette vente annulée à la dernière minute par le propriétaire.
Si la Cour d'appel rejette cette demande[354], cet avis n'est, certainement, pas celui partagé par la Cour de cassation qui casse l'arrêt rendu par la Cour d'appel[355], au visa de l'article 1583 du Code civil.[356]

Cette décision, qui n'est pas sans rappeler une affaire similaire déjà jugée par la 1ere chambre civile de la Cour de cassation en 1991[357], démontre que le principe historique du consensualisme est d'actualité et que son utilisation n'a pas vocation à s'estomper. Bien au contraire, la référence au consensualisme et par là le renforcement de celle de consentement ne cesse de s'accroitre ces notions allant, actuellement, de pair avec l'utilisation exponentielle des données personnelles.

107. Par-delà l'approche historique, il convient de s'intéresser, plus en profondeur à la notion propre de consentement tel qu'elle subsiste, actuellement, en droit civil et surtout en droit des contrats.

Le contrat est compris comme un accord de volonté destiné à produire des effets relatifs d'obligations[358]. Or, pour produire cet effet, il doit, aux termes de l'article 1103 du Code civil, être « *légalement formé* »[359]. C'est-à-dire, qu'il doit respecter

---

354 « E*n estimant que le mandat confié à la société n'était en rien un engagement certain de vente de la part du propriétaire et que l'acceptation ultérieur, sans aucune autre précision sauf la mention « bon pour accord », de l'offre d'achat à un prix inférieur à celui convenu dans le mandat n'emportait pas acceptation définitive du propriétaire* », URL : https://www.legavox.fr/blog/lajurisprudence/solus-consensus-obligat-consentement-oblige-19079.htm

355 Décision attaquée : Cour d'appel d'Aix-en-Provence, du 18 février 2014.

356 « *Une offre d'achat qui désigne la chose et mentionne le prix vaut vente dès lors qu'elle a été acceptée sans réserve ; que la Cour d'appel n'a pas relevé que X avait émis des réserves en acceptant l'offre litigieuse ; que des lors, en énonçant que l'accord de X portait sur « l'acceptation de l'offre en tant que telle » mais n'impliquait pas « l'engagement de vendre », la Cour d'appel a violé l'article 1583 du Code civil* », Cass. civ. 3e, 12 novembre 2015, 14-17.790, Inédit.

357 Cass. civ. 1ere, 2 juillet 1991, n°90-10187.

358 C. civ., art. 1101, *préc.*

359 *« Les contrats légalement formés tiennent lieu de loi à ceux qui les ont faits* », C. civ., art. 1103 (*Ord. nº 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

les conditions que la loi exige pour sa validité, à tel point que, si ces exigences ne sont pas respectées, la sanction, en principe, en est la nullité[360].

Dans l'ancienne version du Code civil, les conditions de validité du contrat étaient énoncées à l'article 1108 ancien, au nombre de quatre, à savoir, « *consentement de la partie qui s'oblige* », « *capacité de contracter* », « *objet certain qui forme la matière de l'engagement* » et « *cause licite dans l'obligation* »[361].

Désormais, les conditions de validité du contrat sont énumérées à l'article 1128 nouveau du Code civil et ne sont plus qu'au nombre de trois, « *consentement des parties* », « *capacité de contracter* » et enfin « *contenu licite et certain* »[362].

Depuis l'Ordonnance, si le consentement et la capacité des parties sont toujours exigés, en revanche, la référence à la cause du contrat est substituée par la référence à son contenu. Le remplacement de la notion de cause à celle de contenu s'explique par deux hypothèses. La première est que la substitution de ces termes est un emprunt, sinon une référence à l'article 13 du projet Terré. La seconde repose sur un souci infiniment plus pratique ou pragmatique. En effet, en abandonnant la vieillissante notion de cause, le nouveau Code civil, par-là réformé, s'inscrit dans une démarche de modernisation, visant ainsi à ce qu'il redevienne un modèle d'antan, tel que l'était le Code de 1804, et puisse s'exporter hors des frontières nationales, notamment en vue d'une possible harmonisation européenne du droit des contrats[363].

---

360 *« Un contrat qui ne remplit pas les conditions requises pour sa validité est nul. La nullité doit être prononcée par le juge, à moins que les parties ne la constatent d'un commun accord. Le contrat annulé est censé n'avoir jamais existé(…)»,* C. civ., art. 1178 (*Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

361 C. civ., anc. art. 1108 *(Abrogé par Ord. n° 2016-131 du 10 févr. 2016, à compter du 1er oct. 2016)*.

362 C. civ., art. 1128, *préc.*

363 *« La perspective d'un droit européen des contrats unifié s'éloigne donc pour l'instant ; elle aura eu au moins un mérite : servir d'épouvantail et ancrer dans les esprits la nécessité de réformer le droit français des contrats »*, M. Latina, *L'attractivité du droit des contrats : la fonction de modèle*, Blog Réforme du droit des obligations, Éditions Dalloz.

« En conclusion, la compréhension du droit du contrat est très largement commune entre le nouveau droit français issu de l'ordonnance et les travaux européens d'unification de ce droit », L. Grynbaum, *Réforme du droit des contrats : synthèse du droit français et convergence avec le droit européen*, Droit de l'immatériel, Lamy Revue, n°124, Mensuel Mars 2016.

108. Pour que le contrat se forme valablement, il faut, non seulement, que le consentement émane d'individus en mesure d'exprimer un consentement véritable, mais encore, il est nécessaire que le consentement présente certaines qualités.

En effet, contracter ce n'est pas seulement être en capacité de consentir, c'est aussi consentir en pleine connaissance de cause et librement. Autrement dit, le consentement doit, d'une part, être donné par une personne apte à consentir et, d'autre part, ne pas être vicié.

Les individus qui ne sont pas en mesure d'émettre un consentement véritable sont frappés d'une interdiction de contracter seul à travers la règlementation des incapacités. Pour contracter régulièrement et légalement, il faut donc avoir la capacité. En ce sens, l'article 1129 du Code civil prévoit alors que « *Conformément à l'article 414-1, il faut être sain d'esprit pour consentir valablement à un contrat* »[364].

Pour autant, il arrive qu'une personne, tout en étant capable, ne soit pas saine d'esprit au moment de la conclusion de l'acte. C'est alors par le recours aux règles relatives à l'insanité d'esprit que la protection du consentement sera assurée.

La capacité juridique, principe universel selon lequel « *Tout Français jouira des droits civils »*[365] peut être définie comme l'aptitude à acquérir un droit et à l'exercer. Aux termes de l'article 1145 alinéa 1er du Code civil, « *Toute personne physique peut contracter sauf en cas d'incapacité prévue par la loi* »[366]. Il résulte que la capacité est donc le principe, l'incapacité l'exception.

109. Après avoir évoqué l'aptitude à consentir, il convient de se demander ce qu'il en est de l'intégrité du consentement ?

Le Code civil fait une large place aux vices du consentement, laquelle découle directement de l'autonomie de la volonté. Dès lors que la volonté est la source du contrat, il est nécessaire qu'elle représente certaines qualités.

---

364 C. civ., art. 1129 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

365 C. civ., art. 8 (*L. 26 juin 1889*).

366 C. civ., art. 1145, al. 1er *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

Pour autant, les rédacteurs de 1804 ont eu conscience de ce que la prise en considération de la seule psychologie des contractants aurait conduit à une grande insécurité juridique. En effet, en tenant en compte de tout ce qui est susceptible d'altérer le consentement, une instabilité dans les rapports contractuels aurait été introduite.

L'impératif de sécurité juridique suppose donc de ne pas prendre en considération toute anomalie, sous peine d'anéantir quasi systématiquement les contrats. C'est ainsi que, tout en réservant une place importante aux vices du consentement, le Code civil n'a admis qu'à des conditions précises qu'ils puissent entrainer la nullité du contrat.

Les règles de droit relatives aux vices du consentement n'ont été que peu modifiées par la réforme qui n'a fait que les enrichir de quelques précisions. L'article 1130 nouveau du Code civil dispose ainsi, conformément à l'ancien article 1109, que « *l'erreur, le dol et la violence vicient le consentement lorsqu'ils sont de telle nature que, sans eux, l'une des parties n'aurait pas contracté ou aurait contracté à des conditions substantiellement différentes* »[367].

Les vices du consentement sont donc au nombre de trois. Pour éclairer le texte précédemment cité, lorsqu'il y a erreur ou dol, le consentement n'a pas été donné en connaissance de cause, lorsqu'il a été extorqué par violence, il n'a pas été donné librement, ce qui, finalement, relève d'une autre logique.

110. Afin de résumer l'analyse classique propre au consentement, il suffit d'avoir bien en tête que contracter c'est être apte à consentir, et consentir en pleine connaissance de cause et surtout librement.

[367] C. civ., art. 1130 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

§2 L'obligation d'information spécifique en lien avec ce consentement

111. L'originalité et la singularité sont des qualités propres de la donnée personnelle qui nécessitent, dans l'intérêt de celle-ci, l'expression d'un consentement affirmé (A) et imposent, du fait de son caractère sophistiqué, la délivrance d'une obligation précontractuelle d'information (B).

A) L'expression d'un consentement affirmé

112. Tandis que le proverbe français « *qui ne dit mot consent* », reprise de la célèbre maxime latine du Pape Boniface VIII (1235-1303), « *qui tacet consentire videtur* »[368], développe l'idée selon laquelle si quelqu'un ne se manifeste pas, qu'il reste silencieux face à une décision ou à une parole, il donne implicitement son accord, cette vérité n'est pas justifiée et n'emporte pas, satisfaction en matière de consentement et d'utilisation de « données personnelles », bien au contraire.

Pour assurer une entière sécurité et protection aux personnes qui mettraient à la disposition d'utilisateurs leurs propres « données personnelles », le règlement général sur la protection des données a pris soin de définir avec précision la notion. Ce dernier estime, en effet, que le consentement de la personne concernée représente « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que les données à caractère personnel la concernant fasse l'objet d'un traitement* »[369].

Quatre conditions doivent donc être réunies pour que le consentement, de la personne concernée, puisse être valablement recueilli. Celui-ci doit, premièrement, être libre, ensuite, spécifique, puis, éclairé et enfin univoque.

---

[368] « *Qui se tait semble consentir* ».

[369] RGPD art. 4, *préc.*

113. Du fait de l'utilisation généralisée de la donnée personnelle, à travers les outils numériques et informatiques, et de la complexité d'une telle mesure, le règlement européen a, pour ce faire, clarifié une méthode d'acceptation et de validité du consentement, lequel pour ce faire *« notamment en cochant une case lors de la consultation d'un site internet »*[370].

S'il est acquis que la seule forme valable pour recueillir un consentement, en ces modalités, soit celle de la « case à cocher », il est, en revanche, certain que le consentement sera renforcé si les enjeux en présence sont risqués.

114. Attention toutefois, les moyens utilisés pour recueillir le consentement des individus, au travers du système de « case à cocher », doivent se conformer à certaines exigences et restrictions. Cette mise en garde fait écho à l'affaire, récente, des compteurs « Linky » du 11 février 2020 par laquelle la commission nationale informatiques et libertés faisait un rappel des règles applicables en la matière.

En effet, à la suite d'un contrôle, cet organe mettait en demeure les sociétés EDF et ENGIE[371] pour non-respect de certaines conditions propre au recueil du consentement concernant les données de consommation issues des compteurs communicants. Il a été, notamment, constaté une méthode de consentement global[372], ce qui est, fortement, contraire aux exigences classiques du Règlement européen.

Une autre affaire, qui concerne, également, la problématique des « cases à cocher ou cases cochées », a été examiné par la Cour de justice de l'Union européenne en novembre 2020, preuve que cette méthode de consentement n'intéresse pas seulement la France.

---

[370] RGPD consid. 32, *préc.*

[371] Décision n° MED 2019-035 du 31 décembre 2019 mettant en demeure la société ELECTRICITE DE FRANCE (EDF).

[372] « *EDF et ENGIE recueillent par le biais d'une seule et unique case à cocher le consentement pour deux opérations clairement distinctes : l'affichage dans l'espace client des consommations quotidiennes et l'affichage des consommations à la demi-heure* », URL : https://www.cnil.fr/fr/edf-et-engie-mises-en-demeure-pour-non-respect-de-certaines-conditions-de-recueil-du-consentement

Par le présent arrêt, qui s'inscrit dans la droite ligne, déjà posée en 2019 par l'arrêt Planet49[373], « *la Cour de justice de l'Union européenne réitère sa position sur l'utilisation de cases cochées par défaut pour recueillir le consentement au traitement de données à caractère personnel* »[374].

Si l'arrêt précédent avait rendu une décision concernant l'utilisation et la captation de consentement par le moyen de « cookies »[375], l'affaire Orange Romania SA était l'occasion pour la deuxième chambre de la Cour de justice de l'Union européenne de rappeler, à propos de contrat cette fois, que n'emporte pas validité le consentement qui se réfère à une clause, déjà cochée par le responsable de traitement[376].

Ces quelques exemples démontrent, sans en amoindrir l'intérêt, que le système de « case à cocher » ne doit tronquer le consentement à obtenir mais doit plutôt permettre de renforcer le sentiment de sécurité que tout individu doit pouvoir attendre lorsque la question de ses données personnelles est en jeux. Ces affaires mettent, au surplus, en lumière le travail réalisé par les organismes tel que la Commission nationale de l'informatique et des libertés, mais aussi par la justice, notamment ici, européenne, afin de faire respecter l'application du règlement et ainsi garantir la protection des données personnelles des individus.

115. Concernant le consentement renforcé, au sujet des enjeux risqués, cela fait naturellement lien avec l'importance de chaque donnée personnelle et revient alors à se pencher sur le principe de l'obligation d'information.

---

373 CJUE, 1er oct. 2019, aff. C-673/17.

374 C. Crichton, *Données personnelles et cases pré-cochées : toujours un défaut de consentement*, Dalloz actualité, 01 décembre 2020.

375 Procédé utilisé par les sites internet qui, à l'aide de petits fichiers, enregistre les informations concernant les utilisateurs tel qu'un pseudonyme, un âge ou encore les préférences et habitudes de navigation.

376 « *Un contrat relatif à la fourniture de services de de télécommunications qui contient une clause selon laquelle la personne concernée a été informée et a consenti à la collecte ainsi qu'à la conservation d'une copie de son titre d'identité à des fins d'identification n'est pas de nature à démontrer que cette personne a valablement donné son consentement, au sens de ces dispositions, à cette collecte et à cette conservation,* ***lorsque la case se référant à cette clause a été cochée par le responsable du traitement des données avant la signature de ce contrat*** », CJUE, 11 nov. 2020, Orange Romania SA, aff. C-61/10.

En effet, quoi de plus simple pour un contractant que d'exposer clairement à son co-contractant, dans le but de mettre en confiance ce dernier, ce qu'il compte faire de ses données personnelles. Après tout, il suffit pour le responsable de traitement, dénué de toute intention malveillante et malhonnête, d'afficher clairement la démarche qui est sienne, dans une perspective de confiance avec ses interlocuteurs, afin d'inciter ces derniers à consentir à l'exploitation de leurs données personnelles.

La personne concernée doit, de prime abord, simplement manifester de façon claire et volontaire, le fait qu'elle acquiesce, délibérément, à la mise à disposition de ses « données personnelles ». Mais pour cela, encore faut-il que la personne concernée sache pourquoi ses « données personnelles » sont collectées et ce qu'il en sera fait. C'est ici toute la question de l'obligation d'information préalable au consentement.

116. Autrefois, l'idée dominait que, sauf obligation légale précise, aucun des contractants n'avait à renseigner son partenaire sur les tenants et les aboutissants du contrat qu'ils envisageaient de conclure. En vertu du principe de l'autonomie de la volonté[377] qui présuppose que les hommes sont libres, égaux et responsables, chacun devait s'informer soi-même sur la portée de ses engagements.

Mais la considération que l'inégalité dans l'information peut entacher l'intégrité du consentement et de ce fait nuire à l'équilibre contractuel a, peu à peu, poussé la jurisprudence à consacrer, dans certaines circonstances, une obligation précontractuelle d'information contraignant celui qui sait ou devait savoir à diffuser l'information à son futur partenaire contractuel.

[377] La théorie de l'autonomie de la volonté est un courant de pensée philosophique, dont la paternité est attribuée à Kant, ayant fortement inspiré les rédacteurs du Code civil en 1804.
« *L'autonomie de la volonté est le principe unique de toutes les lois morales et des devoirs qui y sont conformes* », E. Kant, *Critique de la raison pratique*, 1788.

B) La délivrance d'une obligation précontractuelle d'information

117. Si l'expression d'un consentement affirmé est l'étape qui valide, en aval, la sincérité de l'accord donné par la personne concernée au responsable de traitement, celle-ci n'est rendue possible que parce que, en amont, une obligation précontractuelle d'information a été délivrée en ce sens.

118. L'obligation précontractuelle d'information *stricto sensu*, règle d'ordre public[378], est désormais consacrée, aux conditions dégagées par la jurisprudence, à l'article 1112-1 du Code civil qui dispose, en son alinéa 1er, que « *Celle des parties qui connait une information dont l'importance est déterminante pour le consentement de l'autre doit l'en informer dès lors que, légitimement, cette dernière ignore ou fait confiance à son cocontractant* »[379]. Une telle obligation, qui s'applique pour des situations diverses et variées, exige, par exemple, le fait que « *Le fabricant d'un produit doit fournir tous les renseignements indispensables à son usage et notamment avertir l'utilisateur des précautions à prendre lorsque le produit est dangereux* »[380], mais impose, également, que, « *Le vendeur d'un produit très récemment commercialisé a l'obligation de donner à l'utilisateur, dont les juges du fond apprécient souverainement le degré de connaissance, tous renseignements utiles pour sa mise en œuvre* »[381].

L'entrave à cette obligation d'information a pour conséquence d'entrainer la responsabilité de celui qui commet une telle faute, comme à vocation de le préciser, en ses termes, la chambre commerciale de la Cour de cassation à propos d'une banque[382].

---

[378] « *Les parties ne peuvent ni limiter, ni exclure ce devoir* », C. civ., art. 1112-1 al. 5 (*Ord. nº 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016*).

[379] C. civ., art. 1112-1 al. 1er (*Ord. nº 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016*).

[380] Cass. civ. 1er, 14 déc. 1982 : *Bull. civ. I, n° 361 ; RTD viv. 1983. 544, obs. Durry*.

[381] Cass. civ. 1er, 4 mai 1994, n° 92-13.377 P.

[382] « *Faute d'une banque qui a manqué à son obligation d'informer en ne mettant pas son client en mesure d'apprécier les conséquences, sur son en engagement personnel, de la modification du projet initial intervenue dans la précipitation et la confusion* », Cass. com., 3 déc. 2013, n° 12-23.976, P : D. 2013. 2908.

119. Aussi, puisque la question de la mise à disposition des « données personnelles » est une information « *dont l'importance est déterminante pour le consentement* », le Règlement européen impose, dès lors, une information concise, transparente, compréhensible et aisément accessible pour les personnes concernées.

Insérés dans le Chapitre 3 du règlement européen relatifs aux « Droits de la personne concernée », les articles 12, 13 et 14 traitent respectivement de la « *Transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée* »[383], de l'« *Information à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée* »[384] et de l'« *Information à fournir lorsque des données à caractère personnel n'ont pas été collectées auprès de la personne concernée* »[385].

La transparence permet aux personnes concernées de connaitre la raison de la collecte des différentes données les concernant, de comprendre le traitement qui en sera fait et d'assurer la maitrise de leurs données, en facilitant l'exercice de leurs droits.

La transparence contribue, en outre, pour le responsable de traitement à un traitement loyal des données et permet d'instaurer une relation de confiance avec les personnes concernées.

A travers de l'article 12, le Règlement rappelle qu'à l'occasion d'un traitement de données, la personne concernée doit recevoir une information délivrée « *de façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples* »[386]. Il ne sera donc pas possible pour le responsable de traitement de noyer toute demande de collecte dans des conditions générales d'utilisation ou dans une flottée de questions, ces astuces étant interdites.

120. Il faut bien comprendre que l'obligation d'information est une véritable mise à disposition du responsable de traitement aux personnes concernées. C'est

[383] RGPD art. 12, *préc.*

[384] RGPD art. 13, *préc.*

[385] RGPD art. 14, *préc.*

[386] RGPD art. 12 al. 1er, *préc.*

un service qu'il faut convient d'assurer, et cela du mieux possible, au risque de voir le consentement donné remis en question par manque d'éléments fournis.
Il ne suffit pas, simplement, pour un responsable de traitement d'avertir ou de mettre en garde les individus, il est important qu'il donne toutes les informations possibles permettant de mettre l'utilisateur dans les meilleures dispositions. L'exemple d'une récente mise en demeure, émanant de la Commission nationale de l'informatique et des libertés adressée au plus haut niveau de l'État, démontre l'autorité et l'irréprochabilité d'une telle obligation. Cette mise en demeure du 15 juillet 2020 reproche au Ministère des solidarités et de la santé certains manquements, notamment vis-à-vis de la pertinence et de la précision des informations fournies[387], en rapport avec l'application StopCovid lancée il y a peu par le Gouvernement[388].

121. En ce sens, l'obligation d'information se détache d'un principe voisin, mais tout aussi essentiel, à savoir le droit d'accès, la mise en œuvre de ce dernier ne nécessitant pas de demande spécifique de la part de la personne concernée. Si ces deux possibilités ont le même objectif, celui d'éclairer la personne concernée au sujet de ces données personnelles, l'obligation d'information s'effectue par le responsable de traitement, alors que le droit d'accès est employé par le véritable titulaire des données.

Le droit d'accès est prévu par l'article 15 du règlement protecteur des données personnelles, il permet pour la personne concernée 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 ainsi que les informations suivantes (...)* »[389]. Cette possibilité renforce la maitrise de ses données personnelles, il est possible, à tout

---

387 « *La Présidente estime que l'information fournie est pour l'essentiel conforme au RGPD. Elle estime cependant que, sur un point, l'information fournie sur les catégories de destinataires des données est incomplète* », Décision n° MED-2020-015 du 15 juillet mettant en demeure le ministère des solidarités et de la santé.

388 « *Les informations sont accessibles dans une rubrique dédiée sur l'application. Elles ne mentionnent toutefois pas l'existence de l'Institut national de recherche en sciences et technologies du numérique (INRIA), sous-traitant, en tant que dentinaire des données, ce qui contrevient à l'article 13 du RGPD* », C. Crichton, *StopCovid : mise en demeure de la CNIL*, Dalloz actualité, 28 juillet 2020.

389 RGPD art. 15 al. 1er, *préc.*

moment, de savoir si tel ou tel organisme détient des informations à son sujet et surtout de savoir s'il s'en sert. Pour user de ce droit, il suffit d'identifier l'organisme en question et de formuler à ce dernier une demande de droit d'accès, étant précisé que la réponse communiquée devra se faire « *dans un format compréhensible* »[390]. Ce mécanisme, qui protège et rassure les individus, vient finaliser l'obligation d'information prévue par les articles précèdent.

Tant l'obligation d'information que son corollaire, le droit d'accès, représentent des principes essentiels que les responsables de traitement ne doivent pas négliger.

122. Toujours dans cette idée de responsabilité, cher au Règlement européen, le responsable de traitement devra, pouvoir être en mesure de démontrer que la personne a donné son consentement, donc, prouver que le consentement a bien été acquis (*cf. article 7 RGPD*)[391], mais également que la personne pourra « *retirer son consentement à tout moment* »[392]. Concrètement, concernant le consentement, il devra être aussi « *simple de retirer que de donner* »[393].

L'article 7 *in fine* du Règlement sur la protection des données est intéressant en ce qu'il traite de l'exécution d'un contrat subordonnée au consentement de la personne, alors que celui-ci n'est pas nécessaire. Une telle démarche ferait état que le critère de la liberté ne serait pas présumé avoir été respecté.
Aussi lorsqu'un responsable de traitement aurait pour souhait, malveillant, d'accaparer des « données personnelles », il devra néanmoins requérir « *un acte positif clair* » afin de s'assurer que la personne concernée « *manifeste de façon libre, spécifique, éclairée et univoque son accord* ». Pour le dire autrement, en cas de silence de la personne concernée, en cas de case « pré-cochées », par défaut, par le responsable de traitement, ou encore, en cas d'inactivité durant un laps de temps, le consentement ne sera point valide.

---

[390] URL : https://www.cnil.fr/fr/le-droit-dacces-connaitre-les-donnees-quun-organisme-detient-sur-vous

[391] RGPD art. 7, *préc.*

[392] RGPD art. 7 al. 3 *in limine*, *préc.*

[393] RGPD art. 7 al. 3 *in fine*, *préc.*

123. En tout état de cause, il est certain qu'obligation d'information et consentement vont de pair avec la mise à disposition des « données personnelles ».

Pour autant, il n'est pas impossible d'émettre une critique quant au consentement donné malgré le respect des différentes obligations et conditions que rencontrent les organismes qui interceptent les données personnelles.

Ainsi, une personne pourra-t-elle donner un consentement au contrat portant sur les données personnelles, conformément aux exigences prévues, à cet effet, sans pour autant que celui-ci soit parfait.

Le consentement donné pourrait l'être d'une manière équivoque, consciente, libre mais également soumise. Il serait alors difficile de déclarer un tel comportement, un tel consentement comme nul puisque celui-ci remplirait, avec rigueur, toutes les obligations qui lui incombent.

En effet, il n'est pas rare de se rendre sur un site et de devoir consentir à la mise à disposition de ses données personnelles afin de pouvoir visiter certains contenus. Ou alors, il est très fréquent, voir automatique, de devoir renseigner ses données personnelles sur un site en étant obligé de créer un compte pour acheter des produits ou bénéficier d'offres spéciales. Bien sûr, il est tout à fait possible de refuser, personne ne force les utilisateurs. Pour autant, c'est une demande de consentement forcée ou déguisée.

Ces diverses situations sont regrettables puisqu'en apparence le consentement donné n'est pas nul car il respecte toutes les obligations imposées par le règlement européen.

124. Si la Commission nationale informatique et libertés ou encore la Cour de Justice de l'Union européenne ont pour mission de contrôler la bonne mise en pratique du règlement européen, il est difficile, en pratique, de tout vérifier.

Pour autant, il convient toutefois de se réjouir du rôle du règlement et de ces institutions puisque si elles ne peuvent pas vérifier toutes les infractions, elles offrent aux individus qui mettent à disposition leurs données personnelles des mises en garde, des outils afin de se protéger.

Si quelques réticences peuvent apparaitre, le consentement des individus aux contrats portant sur les données personnelles elles-mêmes reste tout de même une condition non négligeable et un moyen de protection pour les données. Encore une fois, c'est en ce sens que l'apport du règlement est majeur.

Section 2 : Les contrats portant sur une prestation en lien avec les données personnelles

125. Si les données personnelles sont au centre de certains contrats, il est des situations ou ces dernières n'en sont qu'un composant secondaire. Dans ces cas, les contrats ne sont pas fondés sur la donnée personnelle, mais ils tissent un lien avec celle-ci, l'interaction entre les deux étant inévitables. Il convient dès lors de s'intéresser au consentement en présence de telles hypothèses.

126. Afin d'éviter une casuistique fastidieuse, il est apparu préférable de mettre l'accent sur deux types de conventions où la donnée personnelle, élément accessoire, joue cependant un rôle fondamental : il s'agit d'une part du contrat de travail (Paragraphe 1) et d'autre part du contrat médical (Paragraphe 2).

§1 Consentement et contrat de travail

127. Le contrat de travail est le contrat synallagmatique par lequel les parties, à savoir, l'employeur d'un côté et le salarié de l'autre, figent leurs relations mutuelles de travail, pour le présent et pour l'avenir[394].

Comme toute convention par nature, la conclusion du contrat de travail est soumise aux règles de droit commun prévues par le Code civil en son article 1128 nouveau.

S'il n'est pas vraiment prévu légalement, le contrat de travail est, pour autant, défini par un arrêt de la Cour de cassation du 22 juillet 1954, les Hauts magistrats estimant, en effet, que « *Il y a contrat de travail quand une personne s'engage à travailler pour le compte et sous la direction d'une autre moyennant une rémunération* »[395].

Jurisprudence et doctrine s'accordent, donc, à dire que l'existence d'un contrat de travail se fait par la présence et la réunion de trois éléments, à savoir

[394] « *Le contrat de travail est soumis aux règles du droit commun. Il peut être établi selon les formes que les parties contractantes décident d'adopter* », C. trav., art. L. 1221-1, *préc.*

[395] Cass. soc., 22 juillet 1954, Bull. IV, n°576.

l'accomplissement d'une prestation de travail par le salarié, en échange d'une rémunération par l'employeur et l'existence d'un lien de subordination, élément essentiel.

128. Depuis le 25 mai 2018 et l'entrée en application du Règlement général sur la protection des données à caractère personnel, les données personnelles des salariés font apparaitre un nouvel enjeu pour la politique même des entreprises.

A ce titre, la Commission nationale de l'informatique et des libertés a porté « *plus particulièrement son attention, pour 2018, sur trois grandes thématiques* »[396], à savoir notamment celles relatives aux « *traitements liés aux recrutements* », et donc par-là, la question du consentement de l'utilisation des « données personnelles » pour un contrat de travail.

Il est, tout à fait, normal que le règlement protecteur des données personnelles se préoccupe de ces différentes problématiques en vue de protéger le simple salarié (en tant qu'individu démuni de pouvoir) contre les acteurs de recrutement que sont les employeurs. En effet, avec l'essor de la technologie numérique, le monde du travail ayant suivi le mouvement, de plus en plus d'acteurs de recrutement traitent des « données personnelles » propres aux candidats à l'aune de techniques toujours plus sophistiquées, notamment, par exemple, à travers l'utilisation d'algorithme permettant l'aide au recrutement.

129. Une mise en garde est, toutefois, nécessaire au sujet de l'emploi d'un tel procédé, plus encore lorsque celui-ci concerne un dispositif dont la finalité est le recrutement de salarié. En effet, une telle manœuvre n'est pas anodine est comporte certaines conditions et conséquences, notamment parce que ce procédé est assimilé, également dans le domaine juridique, à un principe dit mathématique[397].

---

396 URL : https://www.cnil.fr/fr/quelles-thematiques-prioritaires-et-quelle-strategie-de-controle-pour-2018

397 URL : https://www.avocats-mathias.com/propriete-intellectuelle/algorithmes-quelle-protection

Une telle conclusion est rendue possible par l'observation de la définition légale présentant l'algorithme comme *« l'étude de la résolution de problèmes par la mise en œuvre de suites d'opérations élémentaires selon un processus défini aboutissant à une solution »*[398].

Puisque l'algorithme est un procédé qui fonctionne « *selon un processus défini* », il faut, pour ce faire, une intervention extérieure afin de pouvoir le programmer avant qu'il n'agisse librement ensuite. L'intervention extérieure est donc celle de l'humain, de l'employeur, qui organise et planifie ledit algorithme à sa guise.

130. Aussi, si l'algorithme est un formidable outil, il n'en reste pas moins un danger pour le recrutement, en cas de mauvaise intention du recruteur. Sur ce point, certains auteurs semblent s'accorder pour dénoncer le fait que « *Un algorithme ''mal nourri'' peut s'avérer très dangereux et aboutir à des abus et des discriminations* »[399]. Pour l'entreprise, utiliser un algorithme, pour faciliter le recrutement, est un gain de temps assuré, néanmoins, il peut y avoir un contrecoup notamment parce que l'algorithme est programmé et à ce titre il n'a aucune marge de manœuvre. Si une société cherche un profil particulier de candidat avec des compétences bien spécifiques, l'algorithme passera à côté de candidats qui n'ont peut-être pas les qualités requises mais qui ont une créativité, une diversité, en plus. Le risque pour l'entreprise est donc d'occulter, par l'utilisation de ce procédé, la dimension humaine pourtant utile à son bon fonctionnement. La première difficulté rencontrée par l'utilisation d'algorithme pour le recrutement est le fait de se retrouver qu'avec un seul profil de candidat, monotone et non atypique. La seconde difficulté et dangerosité pour l'entreprise est celle de répéter les fautes commises. En effet, si une entreprise utilise son ancienne base de données pour calibrer l'algorithme, il est certain que celui-ci renouvellera les erreurs de casting passées[400].

---

[398] Art. 3, Annexe 1, Arrêté du 27 juin 1989 relatif à l'enrichissement du vocabulaire de l'informatique.

[399] URL : https://www.svp.com/article/algorithme-et-data-opportunite-et-danger-pour-le-recrutement-100010488

[400] C. Crichton, *Algorithme et personnalité numérique*, Dalloz actu étudiant, 25 avril 2019.

131. Pour une meilleure compréhension, de la problématique en question, il faut avoir en mémoire, le remarquable principe de non-discrimination érige au sein de l'article L. 1132-1 du Code du travail[401].

Concrètement, en pratique, l'employeur, qui utilise un tel mécanisme, afin de faciliter sa recherche de futur salarié, doit être attentif aux paramétrages qu'il emploie afin de respecter les conditions prévues par le texte précité et ne soit pas accusé d'une quelconque manœuvre discriminatoire, qui serait intentionnelle ou non-intentionnelle.

Si le risque de discrimination est présent, notamment parce que cette méthode a pour objectif celui de s'informer, au maximum, sur le candidat et potentiel salarié, elle n'en reste pas pour le moins légalement possible. Le but, légitimement poursuivi, étant pour les employeurs de collecter le plus d'informations possible sur le postulant afin de savoir si ce dernier sera en adéquation avec le travail demandé.

Ainsi, par la collecte d'une multitude de données à caractère personnel concernant le (futur) salarié, il sera possible pour l'employeur d'analyser le profil et les compétences de ce dernier, ses qualités ou encore ses défauts, et donc sa capacité à occuper le poste à pourvoir.

132. Juridiquement, le Règlement général sur la protection des données prévoit et admet que le traitement des « données personnelles » recueillies auprès des salariés d'une entreprise sera conforme, si et seulement, s'il repose sur l'un des

---

401 « *Aucune personne ne peut être écartée d'une procédure de recrutement ou de l'accès à un stage ou à une période de formation en entreprise, aucun salarié ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte (…) en raison de son origine, de son sexe, de ses mœurs, de son orientation sexuelle, de son identité de genre, de son âge, de sa situation de famille ou de sa grossesse, de ses caractéristiques génétiques, de la particulière vulnérabilité résultant de sa situation économique, apparente ou connue de son auteur, de son appartenance ou de sa non-appartenance, vraie ou supposée, à une ethnie, une nation ou une prétendue race, de ses opinions politiques, de ses activités syndicales ou mutualistes, de son exercice d'un mandat électif de ses convictions religieuses, de son apparence physique, de son nom de famille, de son lieu de résidence ou de sa domiciliation bancaire, ou en raison de son état de santé, de sa perte d'autonomie ou de son handicap, de sa capacité à s'exprimer dans une langue autre que le français* », C. trav., art. L. 1132-1.

fondements prévus par l'article 9 qui traite du traitement portant sur des catégories particulières de données à caractère personnel[402].

Si le règlement impose le respect d'une liste limitative pour recueillir en toute conformité les « données personnelles » des salariés, le consentement de ces derniers au traitement de leurs données à caractère personnel n'est pas pour autant un principe inébranlable. A tel point qu'une expertise de la situation laisse à prétendre que, « *Le consentement des salariés n'est pas nécessaire, ni pertinent !* »[403].

133. Le principe, développé depuis la mise en œuvre du Règlement européen, selon lequel tout traitement de données à caractère personnel doit obligatoirement reposer sur le consentement exprès des personnes dont les données sont traitées, n'est pas toujours incontestable. Le sacro-saint « consentement » peut, par exemple, connaitre quelques contrariétés en matière de mise à disposition de « données personnelles » et de contrat de travail.

Tout d'abord, sur le plan pratique, l'absence de consentement, donc le refus du salarié à consentir à l'utilisation de ses propres « données personnelles » neutraliserait le bon fonctionnement du contrat de travail et par la même l'entreprise à laquelle il est lié. Il parait en effet dangereux que cette relation à double sens, ce contrat synallagmatique, qu'est le contrat de travail, puisse être paralysé par un salarié qui refuserait de délivrer quelques informations sur sa personne, alors que certaines informations sont à la fois nécessaires pour l'entreprise et sans aucun risque pour ce dernier.

---

[402] « *a) La personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, c) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, d) le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, e) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée, f) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur* », RGPD art. 9, *préc.*

[403] URL : https://www.village-justice.com/articles/rgpd-donnees-consentement-des-salaries-est-pas-necessaire-pertinent,30337.html

Sur le plan juridique, ensuite, le Groupe de travail « Article 29 » sur la protection des données ou « G29 » considère que le consentement peut s'avérer, partiellement, offensé en raison du « *déséquilibre des rapports de force ayant lieu dans le cadre des relations de travail* »[404].

A ce titre, ledit règlement prévoit, pour faire face à cette faiblesse, à l'article 88 que « *Les États membres peuvent prévoir, par la loi ou au moyen de conventions collectives, des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des employés dans le cadre des relations de travail, aux fins, notamment, du recrutement, de l'exécution du contrat de travail* »[405].

Cette marge de manœuvre traduit la difficulté d'associer le consentement à l'utilisation des « données personnelles » et les relations de travail. En effet, aux vues de la délicate relation employeur/employé, il n'est pas certain que la personne concernée (en l'espèce un salarié) soit en mesure de pouvoir refuser le consentement qu'il doit donner à son employeur.

134. Aussi, ce même « G29 » avançait un début de réponse à cette problématique en estimant légitimement que « *les employeurs traitent des données à caractère personnel de leurs employés en se fondant sur leur consentement, dès lors qu'il est peu probable que celui-ci soit donné librement* »[406]. Dire cela ne signifie pas que l'employeur puisse passer outre le consentement des salariés, mais cela démontre qu'en matière de relation de travail, il ne faut pas oublier que la relation employeur/employé étant biaisée, pour éviter de la paralyser, il est préférable de véritablement se référer au consentement de l'employé quand cela est profondément nécessaire.

En effet, il ne faut pas redouter que les employeurs s'obstinent à ne jamais demander le consentement de leurs salariés, par crainte de refus ou de paralysie, car il ne faut pas oublier que le règlement européen prévoit plusieurs contrôles qui

---

[404] Groupe 29, *Groupe de travail « article 29 », Lignes directrices sur la transparence au sens du règlement (UE) 2016/679*, WP 259 rev.01, 10 avril 2018, p. 7.

[405] RGPD art. 88, *préc.*

[406] Groupe 29, *Groupe de travail « article 29 », Lignes directrices sur la transparence au sens du règlement (UE) 2016/679*, *préc*, p. 8.

permettront de vérifier la licéité et la conformité des actions menées par une entreprise, en tant que responsable de traitement et utilisateur de « données personnelles ».

Les contrôles répétés de certaines institutions, telles que la « CNIL », permettront de vérifier les moyens déployés pour l'identification de candidats, les outils utilisés par les équipes de recrutement pour leur évaluation, les critères de sélections ou encore les conditions de traitement des données des salariés.
A ce sujet, et puisque déjà évoqué, il ne faut pas oublier que l'article 24 du règlement général sur la protection des données responsabilise les employeurs. En tant que responsable de traitement, ces derniers devant démontrer et prouver que « *le traitement est effectué conformément au présent règlement* »[407]. Si tel n'est pas le cas, gare aux sanctions… !

135. Après avoir examiné la situation de l'obligation au consentement des données personnelles dans le cadre de recrutement, il parait approprié de confronter, également, à cette problématique, l'exemple du télétravail, situation définie à l'article L. 1222-9 du Code du travail[408].
En effet, cette méthode de travail est de plus en plus repandue du fait de l'essor des nouvelles technologies et s'impose, également, en temps de crise sanitaire comme c'est, actuellement, le cas.

Si bon nombre de sociétés, pour ne citer que les « start-up », peuvent se permettre un tel fonctionnement de travail, profitant ainsi de cette occasion pour réduire les charges d'exploitation (notamment locatives), le télétravail ne doit pas, pour autant, être un moyen de négliger les règles régissant la relation employeur/employé.

---

[407] RGPD art. 24 al. 1er, *préc.*

[408] « *Sans préjudice de l'application, s'il y a lieu, des dispositions du présent code protégeant les travailleurs à domicile, le télétravail désigne toute forme d'organisation du travail dans laquelle un travail qui aurait également pu être exécuté dans les locaux de l'employeur est effectué par un salarié hors de ces locaux de façon volontaire en utilisant les technologies de l'information et de la communication* », C. trav., art. L. 1222-9.

Il est alors intéressant d'examiner un exemple, permettant de démontrer que le télétravail doit, au même titre qu'un contrat de travail, respecter les exigences en matière de consentement et de données personnelles des salariés.

136. Une situation parlante représente le cas de « visio-conférence », évènement anodin, mais qui par le contexte de confinements successifs mis en place pour mettre fin à la crise sanitaire lié à la pandémie de Covid19 en devient une expérience qui a son importance. Il est en effet fréquent, en période aménagée de télétravail[409], lorsque l'état d'urgence est déclaré[410], d'utiliser des outils informatiques tel que la visio-conférence, permettant de se réunir à plusieurs et en direct, afin de faciliter les échanges.

Ce procédé, des plus simple, ne doit, toutefois, pas mettre à l'épreuve, ni entraver la vie privée des salariés et doit donc, à ce titre, respecter les données personnelles propres à chacun des utilisateurs, en l'occurrence les employés présents à ce type de réunion par interface numérique.
C'est pourquoi, à propos des cas de visio-conférences, un avertissement[411], plus à prendre comme un conseil qu'en une réelle obligation, est adressé aux employeurs reposant sur le principe de minimisation des données, lui-même, également, consacré par le Règlement général sur la protection des données à l'article 5. 1. c)[412].

137. Le principe de minimisation des données oblige donc aux responsables de traitement, en l'espèce aux employeurs, de privilégier la situation la plus homogène avec lesdites conditions susvisées. Il sera alors souhaitable, pour le cas de visio-conférence de n'utiliser que la fonctionnalité du micro pour échanger

---

409 « *En cas de circonstances exceptionnelles, notamment de menace d'épidémie, ou en cas de force majeure, la mise en œuvre du télétravail peut être considérée comme un aménagement du poste de travail rendu nécessaire pour permettre la continuité de l'activité de l'entreprise et garantir la protection des salariés* », C. trav., art. L. 1222-11.

410 Loi n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19.

411 « *La CNIL recommande aux employeurs de ne pas imposer l'activation de leur caméra aux salariés en télétravail* », URL : https://www.efl.fr/actualites/social/contrat-de-travail/details.html?ref=f0a3c09fb-d3d8-4a50-8a6a-89537f997871

412 « *Les données à caractère personnel doivent être (...) adéquates ; pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* », RGPD art. 5. 1. c), *préc.*

avec les protagonistes, sans allumer de caméra. Si le dispositif du micro permet de suffire aux exigences de l'employeur, alors cette solution doit être celle retenue.

Si une telle revendication peut paraitre pointilleuse, il ne faut pas oublier que l'image d'une personne, plus encore lorsque celle-ci est captée par un outil informatique, fait partie intégrante du champ de ce que sont les données personnelles propres à la personne[413].

La solution, ainsi retenue, est semblable à une décision déjà rendue par la Cour de cassation, au visa de l'article L. 1121-1 du Code du travail[414], à propos de vidéosurveillance, la chambre sociale considérant que « *Un employeur ne peut mettre en place un système de vidéosurveillance que si ce dispositif est justifié par la nature de la tâche à accomplir et proportionné au but recherché* »[415].

Si le consentement donné au contrat de travail par la personne en recherche d'emploi (en phase de recrutement) est un fondement à la formation de celui-ci, l'exécution du contrat en question doit toujours être subordonnée à ce même impératif.

Le cas de l'acceptation ou non de la mise en marche d'une caméra aux fins d'une visioconférence n'échappant pas à la règle précitée, à savoir celle du consentement. L'individu peut alors, par ce moyen, qu'il ne faut pas lui imposer, contrôler son image, donc contrôler ses propres données personnelles.

138. En résumé, il est possible d'énoncer qu'une relation de travail intègre, inéluctablement, la question des données personnelles des salariés. En effet, en pratique, l'employeur aura connaissance de données intimes de personnes, bien avant de s'engager avec elles, par la transmission de *curriculum vitae*, par la réponse à des questionnaires, par l'utilisation d'algorithme ou d'intelligence artificielle. L'employeur devra donc prendre la mesure de l'importance de

---

413 RGPD art. 4, *préc.*

414 « *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* », C. trav., art. L. 1121-1, *préc.*

415 Cass. soc., 20 nov. 1991, n° 88-43.120 *P : D. 1992. 73, concl. Chauvy*.

l’acquisition de ces données et devra les respecter tout au long du fameux contrat de travail.

Il sera désormais pertinent de s’intéresser à cette même relation et des enjeux qui s’y rapportent au travers, cette fois, du contrat médical.

§2 Consentement et contrat médical

139. Si le consentement est un facteur déterminant pour la réalisation de contrat médical dont la donnée personnelle n'est qu'accessoire, cette relation doit s'analyser en situation normale (A), mais également en situation de crise sanitaire (B), pour en mesurer les conséquences.

A) La dépendance du contrat médical au consentement en situation normale

140. C'est par le célèbre arrêt « Mercier » rendu par sa chambre civile le 20 mai 1936 que la Cour de cassation a dégagé une définition du contrat médical en admettant « *qu'il se forme entre le médecin et son client un contrat comportant pour le praticien l'engagement de donner des soins attentifs, consciencieux et, sous réserve faite de circonstances exceptionnelles, conformes aux données acquises de la science* »[416].

En ce sens, le contrat médical est un contrat spécial[417] puisqu'il est le fruit d'une relation médecin/patient dans lequel le professionnel peut voir sa responsabilité engagée par le malade. La responsabilité médicale désigne l'obligation pesant sur les professionnels de santé de réparer le dommage causé par la mauvaise exécution d'un contrat de soins. Les conséquences d'une inexécution contractuelles engagent désormais la responsabilité du professionnel en vertu de la loi[418], l'article L. 1142-1 du Code de la santé publique affirmant, à ce titre, que « *I. – Hors le cas ou leur responsabilité est encourue en raison d'un défaut d'un produit de santé, les professionnels de santé, (…), ainsi que tout établissement, service ou organisme dans lesquels sont réalisés des actes individuels de prévention, de diagnostic ou de soins ne sont pas responsables des conséquences dommageables d'actes de prévention, de diagnostic ou de soins qu'en cas de*

---

[416] Cass. civ. 1, 20 mai 1936, *Mercier : GAJC, 11e éd., n°161-162 (I) ; DP 1936. 1. 88, rapp. Josserand, concl. Matter, note E. P*.

[417] F. Leclerc, *Droit des contrats spéciaux,* 2e éd., Lextenso, LGDJ, 2012, p. 21 et s.

[418] E. Terrier, *Responsabilité medicale, in Responsabilité civile*, Encyclopédie - Répertoire civil, Dalloz, 2020, 104 p.

faute »[419]. Pour autant, le contrat médical demeure et le principe d'une inexécution contractuelle fonde toujours la « faute » au sens de cet article.

141. S'il n'est pas lieu ici de s'attarder sur la responsabilité médicale[420], il parait nécessaire d'analyser un autre principe cher au droit médical, et dans la continuité de la question du consentement, celui de l'obligation d'information.

En effet, bien que désormais également légale, cette obligation d'information à l'origine fondée sur le contrat de soins[421], c'est dorénavant le Code de la santé publique pose le principe de l'obligation d'information, propre au droit médical, à travers l'article L. 1111-2 qui dispose que « *Toute personne a le droit d'être informée sur son état de santé. Cette information porte sur les différentes investigations, traitements ou actions de prévention qui sont proposés, leur utilité, leur urgence éventuelle, leurs conséquences, les risques fréquents ou graves normalement prévisibles qu'ils comportent ainsi que sur les autres solutions possibles et sur les conséquences prévisibles en cas de refus* »[422]. L'alinéa 7 de ce même texte affirme que « *En cas de litige, il appartient au professionnel ou à l'établissement de santé d'apporter la preuve que l'information a été délivrée à l'intéressé dans les conditions prévues au présent article. Cette preuve peut être apportée par tout moyen* »[423]. Il est fort logique que le Code de la santé publique établisse une telle charge de la preuve puisqu' il est aisé pour un professionnel ou un établissement de santé de démontrer que son obligation d'information a bien été remplie par des moyens vérifiables tels qu'une documentation, un formulaire ou une attestation que le patient aurait signé. A l'inverse, il serait impossible pour un patient de démontrer qu'il n'a pas reçu les informations adéquates, le fait de rapporter une absence de preuve étant un non-sens.

---

[419] CSP., L. 1142-1 al. 1er.

[420] *Ibid.*

[421] Cass. req., 28 janvier 1942, *Parcelier c/ Teyssier*, Bergoignan-Esper et Sargos, GADS, Dalloz, 2021, n°1.

[422] CSP., L. 1111-2 *in limine*.

[423] CSP., L. 1111-2 al. 7.

142. Tout comme l'obligation d'information impose aux professionnels de santé d'éclairer le patient afin qu'il consente en connaissance de cause à l'acte de soin en question, le secret médical s'impose également au corps médical, sa transgression est, comme pour l'obligation précédente, lourde de conséquences.

Pour autant, si le Code de la santé publique s'efforce de mettre en avant certains principes forts, tel que celui décrit à l'article L. 1110-4, à savoir celui du secret médical, ces principes semblent, toutefois, en déclin. En effet, le devoir de respect au secret médical est un principe déontologique fondamental, il n'en reste pas moins que la circulation des informations et le partage de celles-ci soit, aussi, une nécessité. Une nécessité médicale avant tout, mais aussi un enjeu financier, permettant, notamment, le contrôle des praticiens-conseils sur les prescriptions effectuées, mais également la mise en œuvre de dispositifs tels que le dossier médical personnel (art. L. 1111-14 s.), censés permettre une meilleure coordination des soins et l'élimination des doublons ou des interactions médicamenteuses.

C'est pourquoi, le III[e] point, alinéa 2, de l'article précité rappelle très clairement cette nécessité, mais pour autant rappelle le devoir de conditionner le partage d'information à la protection de l'information médicale : « *Le partage, entre des professionnels ne faisant pas partie de la même équipe de soins, d'informations nécessaires à la prise en charge d'une personne requiert son consentement préalable, recueilli par tout moyen, y compris de façon dématérialisée, dans des conditions définies par décret pris après avis de la Commission nationale de l'informatique et des libertés* »[424].

143. Puisqu'elles portent sur des données de santé, qui sont des données personnelles, tant l'obligation d'information que sa conséquence, c'est à dire le secret médical, sont de ce fait, soumis, par souci de protection, à des conditions très strictes[425]. Lorsqu'un patient est pris en charge, la circulation des informations le concernant est libre pour l'équipe médicale qui s'occupe de lui. Dès que ce noyau s'élargit, la transmission des données est possible sur format numérique ou

[424] CSP., L. 1110-4, III, al. 2, *préc.*

[425] E. Terrier, *Responsabilité medicale, in Responsabilité civile*, *Op cit*, 104 p.

papier mais elle est soumise à l'approbation du patient. Cela s'impose par exemple à un second médecin et une seconde équipe médicale qui pratiquerait un acte de soin autre que celui déjà réalisé. En élargissant encore un peu plus le périmètre, la transmission de donnée du patient est possible, néanmoins, avec son accord et si elle ne porte que sur des éléments nécessaires. Il s'agira ici de ne divulguer que certaines informations utiles et spécifiques à un kinésithérapeute, par exemple. Cette même restriction doit être respectée lorsque les données personnelles sont transmises à un organisme dont le champ d'action est encore plus éloigné telles que l'assurance du patient ou la médecine du travail.

Les données de santé étant de réelles données personnelles, propres au patient, l'exigence de protection à leur égard est, naturellement, des plus élevées. Pour autant, si le secret médical doit être scrupuleusement respecté, il est des situations, notamment dans l'intérêt exclusif du patient, dans lesquelles il sera possible, voire nécessaire, de divulguer et de transmettre ces informations. Voilà pourquoi des conditions contraignantes s'imposent durant toute la chaine médicale afin de veiller à la sécurité et au respect de celles-ci.

144. Aussi, à l'instar de ce qui est déjà préconisé dans le secteur médical, le Règlement général sur la protection des données semble s'inscrire directement dans le sillage du Code de la santé publique. Cela se comprend aisément tant les « données personnelles » du patient sont ici des informations sensibles, une protection particulière de ces dernières est donc nécessairement bienvenue. Voilà ce que résume l'article R. 4127-35 du Code de la santé publique en exprimant que « *Le médecin doit à la personne qu'il examine, qu'il soigne ou qu'il conseille une information loyale, claire et appropriée sur son état, les investigations et les soins qu'il lui propose* »[426]. Cette démarche, il convient d'entendre par là, ce souci de protection, est d'autant plus conséquent en matière de consentement du patient, dont l'obligation d'information n'est qu'une première étape.

La prestation médicale étant un acte qui peut être invasif et porter atteinte à l'intégrité au corps pour le patient, il est de ce fait naturel qu'il soit lui et lui seul concerné par les prérogatives de la relation contractuelle. L'article L. 1111-4 *in*

[426] CSP., R. 4127-35 al. 1er.

limine du Code de la santé publique traduit parfaitement cette idée puisqu'il suggère que « *Toute personne prend, avec le professionnel de santé et compte tenu des informations et des préconisations qu'il lui fournit, les décisions concernant sa santé* »[427]. Le texte va encore plus loin dans ce raisonnement, puisque à l'alinéa 2 se retrouve le principe selon lequel « *Toute personne a le droit de refuser ou de ne pas recevoir un traitement* »[428]. A noté sur ce point, qu'un tel refus devra être recueilli dans les mêmes conditions que le consentement à un acte de soin, c'est-à-dire que le refus devra être libre et éclairé.

La possibilité de refuser un acte de soin représente pour le patient une situation qui démontre l'importance accordée à ces données. En effet, un tel refus, qui peut avoir des conséquences dramatiques pour le patient, renforce la maitrise personnelle de celui-ci sur ses données. Le patient, au même titre que la personne concernée est seul maitre de son corps, de ses données de santé ou pour le dire autrement de ses données personnelles. Accordant un tel pouvoir au patient, s'est en réalité reconnaitre la primauté de ses données.

Il en va de même concernant l'accès aux « données personnelles » du patient, entendre ici l'accès au dossier médical personnel du patient. L'article L. 1111-7 du Code de la santé publique recouvre, à ce titre, l'idée selon laquelle le patient doit avoir accès à son dossier et cela « à quelque titre que ce soit ».

145. Si ces différents articles ne traitent pas directement du consentement, du patient, à l'utilisation de ses propres « données personnelles », il en résulte tout de même qu'une attention particulière est portée lorsque le contrat, en l'espèce le contrat médical, traite indirectement de l'utilisation des « données personnelles ». Plusieurs parallèles existent en effet entre le Code de la santé publique et le Règlement. Si d'un côté, l'article L.1111-4 alinéa 4 du Code de la Santé Publique précise que « *Aucun acte médical ni aucun traitement ne peut être pratiqué sans le consentement libre et éclairé de la personne et ce consentement peut être retiré à tout moment* »[429], de l'autre, le fameux règlement, comme un miroir, y répond par l'article 7 relatif au consentement, faisant référence à la possibilité pour la

[427] CSP., L. 1111-4 al. 1er.

[428] CSP., L. 1111-4 al. 2.

[429] CSP., L. 1111-4 al. 4.

personne concernée de « *retirer son consentement à tout moment* »[430]. De même, l'article L.1111-7 du Code de la Santé Publique qui prévoit que « *Toute personne a accès à l'ensembles des informations concernant sa santé détenues, à quelque titre que ce soit* »[431] est le corolaire d'un principe inséré dans le Chapitre 3 du règlement européen relatifs aux « Droit de la personne concernée ». Il s'agit tant en droit médical qu'en matière de données personnelles d'une question de transparence à l'égard des informations délivrées par le patient ou la personne concernée. La personne qui dévoile et transmet des informations là concernant peut, à tout moment, en connaitre l'utilisation. En matière médicale la personne divulgue des informations pour le bien de la réalisation d'un acte de soin et peut à ce titre en connaitre les effets (méfaits ou bienfaits). En définitive, le patient peut être informé de l'évolution de sa situation. En matière de données personnelles, la personne qui consent à l'utilisation de ses données peut à tout moment savoir comment et dans quel but celles-ci sont utilisées.

146. Enfin, le rapprochement entre le Code de la Santé Publique et le présent règlement semble évident concernant les notions de charge de preuve et de responsabilité. En effet, le droit médical, à l'aune d'une jurisprudence dégagée par la Cour de cassation dans un arrêt du 25 Février 1997 (puis reprise à l'article L. 1111-2 alinéa 7 CSP), s'est construit autour du principe selon lequel « *le médecin est tenu d'une obligation particulière d'information vis-à-vis de son patient et il lui incombe de prouver qu'il a exécuté cette obligation* »[432]. A noter que l'obligation particulière d'information, dont la finalité est le secret médical, comporte différentes restrictions dont le seul respect permet de s'assurer de la libre transmission des données dans l'intérêt du patient[433].

La question de la preuve, de nos jours, applicable au sens de l'article 24 du règlement protecteur des données personnelles, l'est tant pour le contrat de travail (*cf. supra*) que pour le contrat médical, les professionnels de santé étant devenus pour le Règlement des « *responsable du traitement* » devant ainsi « *être en*

---

[430] RGPD art. 7 al. 3 *in limine*, *préc.*

[431] CSP., L. 1111-7 *in limine*.

[432] Cass. civ. 1ère, 25 février 1997, *Hedreul c/ Cousin et a : Bull. civ. I, n°75, p. 49 ; Gaz. Pal. 1997. 1. 274, rapp. P. Sargos, note J. Guigue*.

[433] E. Terrier, *Responsabilité medicale, in Responsabilité civile*, *Op cit*, 104 p.

mesure de démontrer que le traitement est effectué conformément au présent règlement »[434].

147. Tout comme pour le contrat de travail, consentement et obligation d'information sont nécessaires pour l'utilisation des « données personnelles » lorsque celles-ci sont applicables au contrat médical, qui ne repose pourtant pas, toujours, directement sur ces informations intimes du patient, mais qui les utilise abondamment. Voilà pourquoi règlement européen et Code de la Santé Publique sont aussi voisins, leurs dispositions renforçant la protection faite aux personnes concernées, en l'occurrence les patients.

Le Règlement des données personnelles ne semble pas pour autant fermé, l'article 9 invoquant en effet l'idée qu'il est possible de passer outre le consentement du patient lorsque le traitement porte sur des catégories particulières de données à caractère personnel. Pour cela, le texte préconise à l'alinéa 3 que « *Les données à caractère personnel visées au paragraphe 1 peuvent faire l'objet d'un traitement aux fins prévues au paragraphe 2, point h), si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel* »[435].

148. Toujours au sujet de la problématique du consentement, lorsque celui-ci émane de prestation en lien avec les données personnelles, en l'espèce celle du contrat médical, il s'avère que quelques dérogations sont à souligner.

En effet, après avoir démontré que, plus qu'aucune autre, la matière médicale fait de l'obligation de l'information, de l'importance du secret, ou encore, du respect du consentement, des conditions indispensables tant la prestation de soin est intrusive pour les patients, celles-ci peuvent, toutefois, connaitre, quelques atteintes.

---

[434] RGPD art. 24 al. 1er, *préc.*

[435] RGPD art. 9 al. 3, *préc.*

Il semble opportun ou plutôt nécessaire de préciser que les entorses, à ces principes pourtant bien établis, ne sont que factuelles, partielles et bien entendu ponctuelles.

Une fois encore, il convient d'examiner la problématique en question à travers l'actualité. C'est malheureusement le sujet de la crise mondiale liée au virus SARS-Covid19 qui permet de mettre en évidence les divers bouleversements, notamment à propos de la question du consentement en droit médical.

Sans remettre en question l'importance du consentement des patients, élément fondamental du contrat médical, il existe des situations, des crises, où l'impératif de nécessité admet, mais plus encore, justifie quelques dérogations au principe.

Il convient alors de s'intéresser au consentement aux données personnelles en temps de crise afin de comprendre comment se justifient les rares exceptions possibles. Pour le dire autrement, la question qui se pose serait celle de savoir si la crise peut-elle et doit-elle tout justifier ?

B) La dépendance du contrat médical au consentement en situation de crise sanitaire

149. Par un discours, prononcé le 16 mars 2020, le Président de la République française, Emmanuel Macron, s'était adressé aux français à propos de l'épidémie de coronavirus, annonçant, par la même occasion, la mise en place du premier confinement[436]. C'est ainsi que, quelques jours après, marqué par l'ampleur de cette épidémie, la loi du 23 mars 2020[437] avait pour vocation de créer un chapitre dans le Code de la santé publique dédié à la notion « d'état d'urgence sanitaire ». Celui-ci s'ouvrant par l'article L.3131-12, ainsi rédigé, à savoir « *L'état d'urgence sanitaire peut être déclaré sur tout ou partie du territoire métropolitain ainsi que du territoire des collectivités régies par les articles 73 et 74 de la Constitution et de la Nouvelle Calédonie en cas de catastrophe sanitaire mettant en péril, par sa nature et sa gravité, la santé de la population* »[438].

L'objectif de la loi précitée est de « *faire face à l'épidémie de covid-19* » en instaurant un chapitre qui a « *la particularité de créer un régime juridique temporaire, qui ne pourra s'appliquer que jusqu'au 1er avril 2021* »[439].

Il faut retenir de ce concept d'état d'urgence, qui fait lui-même écho à ce que la jurisprudence appelait déjà en 2008 « l'ordre public sanitaire »[440], qu'il n'a vocation à subsister que pour gérer la crise, parce que la crise existe et seulement durant le temps de la crise.

---

436 « *Nous sommes en guerre, en guerre sanitaire, certes : nous ne luttons ni contre une armée, ni contre une autre Nation. Mais l'ennemi est là, invisible, insaisissable, qui progresse. Et cela requiert notre mobilisation générale* », Adresse aux français du Président de la République Emmanuel Macron, 16 mars 2020, Élysée.

437 Loi n° 2020-290 du 23 mars 2020, *préc*.

438 CSP., L. 3131-12.

439 C. de Gaudemont, *Covid-19 et loi d'urgence : état d'urgence sanitaire*, Dalloz actu étudiant, 24 mars 2020.

440 *« L'ordre public sanitaire se situe au cœur des missions régaliennes. Condition du bon ordre et de la propriété sociale, la protection de la santé publique contribue en effet à la sureté et à la préservation des intérêts fondamentaux de la société qui fondent la légitimité de la puissance publique. L'ordre public sanitaire obéit aussi à un régime juridique bien spécifique. Norme de droit, il contraint les administrés, dont il limite les libertés, et s'impose à l'administration, tenue d'exercer ses prérogatives régaliennes* ». S. Renard, *L'ordre public sanitaire. Étude de droit public interne*, thèse droit, Rennes, 2008.

Cette répétition, est nécessaire pour bien faire entendre que s'il existe un tel régime juridique, comportant certaines conséquences, ce n'est que pour un temps limité, à cause d'une situation exceptionnelle.

Sans remettre en cause l'importance du combat contre le virus, il faut noter que l'orientation et l'administration, en temps de crise, mettent en lumière certaines réalités, notamment concernant des privations de libertés sans précédent, mais aussi des intrusions pour les données intimes de la population[441].

150. Si le confinement ou le couvre-feu sont les restrictions les plus visibles, les fichiers et applications, qui permettent de lutter contre la propagation du virus, représentent, quant à eux, des atteintes, potentielles, à la vie privée, surtout par rapport aux données personnelles (par exemple en cas de fuites de celles-ci)[442].
En effet, afin de lutter contre l'épidémie et pour retrouver une situation sanitaire stable, il est rendu possible, sous certaines conditions et mesures, de porter atteinte aux données de santé, donc aux données personnelles et ce dès aujourd'hui, mais également pour demain.

A court terme, par exemple en pratique, lorsqu'une personne est déclarée atteinte du SARS-Covid19, elle doit, selon l'assurance maladie, « lister les personnes » avec qui elle a eu un contact rapproché. Si la plupart du temps, les personnes « cas contacts » représentent la famille, les amis et les proches, il peut s'agir, en outre, de collaborateurs ou bien plus grave encore de clients. Pour certains

---

441 « *L'état d'urgence sanitaire donne une base légale à un certain nombre de restrictions des libertés au nom de la lutte contre le risque de contagion. Sa manifestation la plus visible en est le confinement. Toutefois, en deux étapes successives, la volonté d'utiliser des informations portant sur la vie privée de la population va s'exprimer puis être introduite dans le droit de crise. Depuis la loi du 11 mai 2020, le covid-19 fait l'objet de la transmission obligatoire des données individuelles à l'autorité sanitaire par les médecins et les responsables des services et laboratoires de biologie médicale publics et privés prévue à l'article L.3113-1 du Code de la santé publique[441]. La violation du secret professionnel, en germe dès le début de la pandémie, va se développer au travers de plusieurs étapes* », B. Py, *Secret professionnel, que n'avons-nous pas retenu de l'expérience du sida ?*, Dalloz actualité, 26 mai 2020.

442 « *Statuant en référé, par remise au greffe le jour du délibéré, après débats en audience publique, par décision contradictoire et en premier ressort, Enjoignons à la SA ORANGE, la SAS FREE, la SA SFR et la SA BOUYGUES TELECOM de mettre en œuvre ou de faire mettre en œuvre, sans délai et pour une période de 18 mois à compter de la présente décision toutes mesures les plus adaptées et les plus efficaces de surveillance ciblées de nature à assurer le blocage effectif du service de communication au public en ligne « XXX » sur leurs réseaux »,* TJ Paris, ord., réf., 4 mars 2021, n° 21/51823.

professionnels, il peut être gênant de divulguer le nom de clients avec qui ils ont été en contact.

Pour l'avenir, la situation actuelle de « data-surveillance » laisse à penser qu'elle sera de plus en plus utilisée et ce, peut-être, même malgré l'absence de crise, ce qui conduira à d'avantages d'atteintes portées aux données, d'autant plus que le pouvoir des géants de l'informatique n'est pas près de s'arrêter, le déséquilibre entre ces plateformes et les personnes concernées s'accentuant de plus en plus[443].

Il suffit de s'intéresser aux fichiers « SI-DEP » et « Contact COVID »[444], ainsi qu'à l'application mobile « TousAntiCovid »[445] (anciennement nommée « StopCovid ») pour se rendre compte de la réalité des faits. La mise en place de tels mécanismes, dont la finalité, respectable, est de limiter la diffusion du virus par l'identification des chaines de transmission, a connu quelques embuches.
C'est par exemple le cas pour l'article 11 de la loi du 11 mai 2020 qui introduit un cas de « dérogation à la dérogation »[446] en autorisant le traitement et le partage des données à caractère personnel concernant la santé relatives aux personnes atteintes par ce virus et aux personnes ayant été en contact avec elles, « *le cas échéant sans le consentement des personnes intéressées* »[447].

---

[443] « *Mais les mesures adoptées sont-elles nécessaires et proportionnées ? Sont-elles au moins utiles à la lutte contre le virus ? L'évaluation de la capacité d'une mesure à combattre un ennemi que l'on connait si mal est, certes, hautement complexe, mais l'absence de débat démocratique n'en demeure pas moins préoccupante, essentiellement pour deux raisons : d'abord, parce que la datasurveillance qui se met en place aujourd'hui risque, par une sorte d'effet cliquet, de perdurer demain ; ensuite, parce que les solutions proposées supposent la collaboration active des géants du numérique et de la techno-surveillance, ce qui n'est évidemment pas sans risque pour la souveraineté numérique* », L. Cluzel-Métayer, *La datasurveillance de la Covid-19*, RDSS 2020, p. 918.

[444] Décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions.

[445] Décret n° 2021-157 du 12 février 2021 modifiant le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid ».

[446] « *En révélant l'état de santé de son patient à un tiers, le médecin est autorisé à violer le secret professionnel (C.pén., art. 226-13) par un nouveau cas de dérogation prévu par l'article 11 de la loi n°2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire* », C. Zorn, *État d'urgence pour les données de santé (II) : sidep et contact covid*, Dalloz actualité, 26 mai 2020.

[447] Art. 11, Loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions.

L'état d'urgence sanitaire impose donc pour une certaine durée quelques entraves, lesquelles sont, justifiées par la nécessité de la situation. Si les plus sceptiques pourront s'offusquer de tels agissements, il convient, pour autant, de saluer ces mesures.

En effet, *a contrario*, que faudrait-il penser si l'État français n'avait pas pris la menace sanitaire trop au sérieux ? S'il est bien entendu, toujours, possible de critiquer les restrictions et mesures dérogatoires en question, parce qu'elles sont très intrusives, très contraignantes, la nécessité de l'urgence peut les justifier.

151. Après avoir démontré que le combat contre la pandémie est une nécessité, ce qui impose à l'État d'agir, notamment par la création d'un état d'urgence sanitaire, permettant de renforcer les prérogatives, qui sont les siennes, il convient de s'intéresser particulièrement à la notion de consentement, mais aussi et surtout à la question du consentement relatifs aux données personnelles. Comment l'état d'urgence sanitaire influe-t-il sur le consentement des patients lorsque la question de leurs données personnelles est en jeux ?

La première façon de combattre le virus est la création de fichiers et d'applications afin de contrôler la chaine de transmission[448], la seconde phase se matérialise par une campagne de vaccination. La question de la vaccination permet de rejoindre les développements précédents, en s'intéressant directement à la question du consentement, cette fois ci, propre au vaccin.

Si la vaccination obligatoire contre le virus du Covid-19 est écartée par le Président de la République[449], il existe, cependant, en France, une liste limitative de vaccins obligatoires[450], instituée par une loi du 30 décembre 2017[451], dérogeant à l'article L. 1111-4 alinéa 4 du Code de la santé publique lequel impose pourtant, pour tout acte médical et traitement, de recueillir le consentement libre et éclaire

[448] Décret n° 2020-551 du 12 mai 2020, *préc* ; Décret n° 2021-157 du 12 février 2021, *préc*.

[449] « *La vaccination doit se faire de manière claire, transparente, en partageant à chaque étape toutes les informations : ce que nous savons, ce que nous ne savons pas. Je veux aussi être clair : je ne rendrai pas la vaccination obligatoire* », Adresse aux français du Président de la République Emmanuel Macron, 24 novembre 2020, Élysée.

[450] CSP., L. 3111-2.

[451] Loi n° 2017-1836 du 30 décembre 2017 de financement de la sécurité sociale pour 2018 (1).

de la personne. Cette liste démontre, une fois encore, que spécifiquement et pour des moments précis, certaines lois dites particulières ou spéciales peuvent porter atteinte et déroger aux lois dites générales, ce qui est le cas en l'espèce puisque « *l'obligation vaccinale, dès lors qu'elle est inscrite dans la loi, prime donc sur le principe du consentement, au nom de la protection de la santé* »[452]. En ce sens, une décision rendue, il y a quelques années par le Conseil constitutionnel, rejetant par là une question prioritaire de constitutionnalité, confortait cette idée en décidant par ces mots que « *les obligations vaccinales sont bien conformes à la Constitution* »[453].

Concernant la question du consentement lorsque les données personnelles sont en jeux, si la vaccination obligatoire est écartée, se pose désormais la question du passeport sanitaire ou passeport vaccinal. Ce procédé n'est-il pas un moyen contourné d'imposer la vaccination au plus grand nombre pour sortir de la crise sanitaire ? Une fois encore, si le bienfait d'une telle mesure n'est pas à remettre en cause et semble donner l'espoir d'un arrêt de l'épidémie, le consentement des personnes concernées apparait bafoué. Si la vaccination n'est en aucune façon coercitive pour la population, certains évènements et déplacements, exigeront, en revanche, d'y recourir. Si le gouvernement ou les autorités n'imposent pas de se soumettre au passeport vaccinal, il s'imposera naturellement, de lui-même, à tous. Pour les plus alarmistes, la création d'un pass-sanitaire[454], en plus d'être liberticide et discriminatoire, représente la porte d'entrée vers l'identification numérique des personnes[455].

Ainsi, l'état d'urgence sanitaire légitime l'effet restrictif, qui existe notamment en matière de liberté, de la politique de santé actuelle, conforme à l'objectif constitutionnel, obligeant le Gouvernement à prendre des mesures drastiques

[452] URL : https://factuel.afp.com/non-une-loi-de-2002-sur-le-consentement-des-patients-ne-permet-pas-deviter-les-vaccins-obligatoires

[453] Décision n°2015-458, QPC du 20 mars 2015.

[454] Loi n° 2021-1040 du 5 aout 2021 relative à la gestion de la crise sanitaire (1).

[455] P. de Villiers, *Le jour d'après*, Albin Michel, 2021, p. 178.

telles que celle du couvre-feu, du confinement de la population ou, plus encore, de l'obligation maquillée de vaccination[456].

Un dernier exemple, concernant le cas de personne souffrant de la maladie tel que celle d'Alzheimer, met en exergue la problématique du consentement au vaccin. Comme cela a été énoncé, plus en amont au sein de cette étude[457], pour consentir il faut réunir deux conditions à savoir, d'une part, comprendre sur quoi repose l'accord à donner et d'autre part, avoir la capacité de donner son accord.
Malheureusement, pour les personnes atteintes de la maladie d'Alzheimer, cette double condition pose des difficultés. Selon une spécialiste du sujet âgé, la réponse à cette situation se décompose en deux temps. En premier, « *chez les malades qui en souffrent, il est préférable de rechercher l'assainissement*[458] ». Enfin, « *Quand la maladie d'Alzheimer progresse et ne permet plus une prise en compte des opinions et des options fondamentales du patient ou de la patiente, on se tourne vers un ''consentement substitué''* »[459].

Si la question du consentement au vaccin n'intéresse pas frontalement celles des données personnelles, il ne faut pas oublier qu'il existe, en aval, différentes hypothèses qui s'imprègnent de celles-ci. Ne faut-il pas s'attendre à ce que les personnes qui se font vacciner fassent l'objet d'un fichier en ce sens, toujours dans le souci de lutter contre la propagation du virus ? Pire encore, ne faut-il pas s'attendre à ce que les personnes qui refusent de se faire vacciner deviennent esclaves de ce choix et ainsi discriminées ?
Voilà en quoi le sujet de la vaccination intéresse particulièrement la notion de données personnelles.

---

456 « *La protection de la santé est un objectif constitutionnel, donc juridiquement, cela justifie qu'on vienne restreindre l'exercice de certaines libertés ou droit fondamentaux. C'est le cas actuellement avec l'état d'urgence sanitaire : la liberté d'aller et venir est constitutionnelle mais elle peut être restreinte pour mener une politique de santé conforme à l'objectif constitutionnel* », J. Peigné interviewé par T. Saint-Cricq, AFP France, *Non, une loi de 2002 sur le consentement des patients ne permet pas d'éviter les vaccins obligatoires*, 2020.

457 V. supra §n°102.

458 Acquiescement déclaré ou tacite à un acte, à une opinion.

459 URL : http://www.slate.fr/story/198715/vaccination-covid-19-maladie-alzheimer-consentement-refuser

152. En définitive, il est loisible d'énoncer que, tout comme la problématique du consentement et du contrat de travail, celle du consentement et du contrat médical recouvre plusieurs difficultés. Cette affirmation n'a de sens que parce que les données collectées, traitées, utilisées sont d'une grande d'importance.

Si le droit du travail et le droit médical s'appuient sur des régimes juridiques spécifiques, il n'en reste pas moins que le Règlement général sur la protection des données personnelles est un atout, majeur, pour la protection des données personnelles.

En effet, pour bien des principes, pour le moins déjà juridiquement tranchés, il est des situations urgentes (en l'occurrence une crise sanitaire) qui chamboulent l'ordre établi et imposent des nouvelles conditions, parfois restrictives, parfois dérogatoires.

C'est donc en cela que le célèbre règlement se doit d'être vigilant, afin de veiller au respect total des données personnelles et ainsi garantir aux personnes concernées une protection la plus sure et complète.

CONCLUSION DU CHAPITRE 1

Le consentement est un élément clé des contrats portant sur la donnée personnelle elle-même ou portant sur une prestation en lien avec celle-ci (contrat médical et contrat de travail).

C'est pourquoi l'importance de cette notion s'apprécie, notamment, à travers l'obligation d'information spécifique lorsque le consentement au contrat donné est en rapport avec la donnée personnelle.

Chapitre 2 : Le consentement à l'utilisation de la donnée personnelle

153. Ce consentement peut être en lien avec le consentement au contrat, qui est l'hypothèse classique (Section 1) ou pas, dans la mesure où le règlement européen établit une distinction entre consentir au contrat et consentir à l'utilisation de la donnée personnelle (Section 2).

Section 1 : Le consentement à l'utilisation de la donnée personnelle est en lien avec le consentement au contrat

154. Après avoir traité de la question du consentement au contrat, qu'il relève directement ou indirectement des « données personnelles », il convient, à présent, d'évoquer l'enjeu qui est celui de consentir avec pour seule finalité l'utilisation de ces dernières.

Si le consentement à l'utilisation de la donnée personnelle bénéficie, en théorie, d'une concordance avec le consentement au contrat (Paragraphe 1), en pratique cette relation perdure également (Paragraphe 2).

§1 Les principes qui fondent cette relation

155. Les deux consentements, à savoir celui propre à l'utilisation de données personnelles et celui relatif au contrat, génèrent par principe des effets semblables qui caractérisent leur similitude. Il convient, dès lors, de s'y intéresser afin de démontrer l'existence d'une relation naturelle entre eux.

D'une part, le consentement, qu'il soit donné pour l'utilisation de données personnelles ou pour la création d'un contrat, est au service des parties et des personnes concernées (A), d'autre part, il semble être un remède nécessaire contre les atteintes subies (B).

A) Le consentement au service des parties et des personnes concernées

156. Si l'un des objectifs qui anime le règlement européen est, en général, mais surtout en ce qui concerne la question du consentement, celui de renforcer le contrôle des personnes concernées[460], cette constance est semblable au principe d'autonomie de la volonté des parties[461], cher au droit des contrats. Il convient, à

[460] RGPD art. 1er, *préc.*

[461] C. civ., art. 1103, *préc.*

ce titre, de rappeler certaines généralités qui démontrent de l'importance du consentement pour ces deux domaines, preuve qu'ils ne sont en rien éloignés, bien au contraire.

157. D'abord créateur d'obligation, le consentement offre, par la suite, aux parties, la possibilité d'user de prérogatives, afin de maitriser l'obligation ainsi créée. Sans le développer, il parait opportun de rappeler le rôle déterminant des parties dans l'élaboration et l'exécution d'un contrat.

Dès la définition même du contrat, la présence et l'importance du consentement se font remarquer, le contrat étant avant tout un « accord de volontés »[462]. Le fait que le consentement des parties représente une des conditions (qui plus est la première) nécessaires à la validité d'un contrat[463] renforce, également, sa position dominante. En droit français, l'idéologie du consensualisme[464] s'impose naturellement et résume à elle seule la théorie de l'autonomie de la volonté et le principe de liberté contractuelle[465] dont le respect à l'ordre public[466] (normes et lois en vigueur) est l'unique limite. La volonté des parties et de ce fait le consentement est donc l'élément originel permettant la création d'un contrat, mais également son interprétation à travers l'intention de celles-ci[467]. Une autre preuve de l'importance accordée au consentement des parties réside dans l'obligation de respecter une délivrance d'informations et ce sans pouvoir ni limiter ni exclure un tel devoir[468]. Puisqu'elles sont intégrées et prises en compte dans le jeu contractuel, les parties, disposent de la possibilité de choisir, comment, sur quoi et avec qui contracter.

En outre, le consentement permet, par la suite, aux parties de veiller à la bonne exécution du contrat, cette manifestation étant annonciatrice d'autre droits et pouvoir que les parties détiennent sur le contrat. La force obligatoire du contrat résume à elle seule l'importance du respect dû aux parties et à leur volonté,

---

462 C. civ., art. 1101, *préc.*

463 C. civ., art. 1128, *préc.*

464 C. civ., art. 1172 (*Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016*).

465 C. civ., art. 1102, *préc.*

466 C. civ., art. 1162, *préc.*

467 C. civ., art. 1188 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

468 C. civ., art. 1112-1 al. 5, *préc*.

puisqu'en effet, si ces dernières ont le pouvoir de créer un contrat, par syllogisme, elles et elles seules ont la possibilité de modifier ou révoquer[469] celui-ci, étant précisé que si l'une des parties ne respecte pas ses engagements, c'est-à-dire si une des parties va à l'encontre du consentement qu'elle a pourtant donné, elle expose le contrat à une sanction, c'est à dire sa nullité[470], preuve une fois encore que la volonté des parties est essentielle.

158. Si l'acte de consentement est la représentation la plus aboutie pour caractériser l'influence des parties sur le contrat, ce processus est également équivalent en matière de données personnelles, preuve qu'un lien existe entre ces deux consentements. En effet, puisqu'à de nombreuses reprises, le Code civil érige, depuis sa rédaction en 1804, la volonté des parties, il est naturel que le règlement général sur la protection des données s'inspire d'une telle considération afin de placer les personnes concernées par l'utilisation de leurs données personnelles au centre de l'attention.

Si le consentement est également au service des personnes concernées par l'utilisation des données personnelles, c'est parce qu'il permet, comme en matière contractuelle, d'ouvrir la voie et l'accès à d'autres droits renforçant ainsi la maitrise sur l'obligation créée, en l'espèce le traitement de données. L'impact d'un tel mécanisme pour le pouvoir des personnes concernées justifie que celui soit encadré et soumis à des conditions très strictes[471].

Outre le fait d'accroitre le pouvoir des personnes concernées sur leurs données, le consentement est un véritable tremplin, une étape obligatoire, vers l'utilisation de nouveaux droits, lesquels ont également pour but, pour les personnes concernées, de suivre l'évolution du traitement mis en place. Le consentement n'autorise pas seulement le traitement de données, il permet pour les personnes concernées d'user de nouveaux droits afin de garder la main mise sur leurs données et ce malgré une « dépossession temporaire » en faveur d'un responsable de traitement.

---

[469] C. civ., art. 1193 (*Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016*).

[470] C. civ., art. 1178, *préc.*

[471] RGPD art. 7, *préc.*

159. Le responsable de traitement doit tout d'abord éclairer la personne concernée en lui délivrant une information spécifique[472] à propos de la collecte de données personnelles en question.

Le consentement permet également d'asseoir l'exigence de sécurité des données propres au règlement européen en mettant à disposition de la personne concernée un véritable droit d'accès[473] sur ses données. Plus qu'une simple information, ou un droit de regard, cette possibilité permet à toute personne concernée, dans la mesure du possible, de demander la consultation de ses données afin de vérifier la licéité des traitements réalisés par le responsable de traitement[474]. Dans le sillage du droit précédent, deux autres facultés se dégagent, à savoir le droit d'obtenir une copie des informations personnelles dont l'utilisation a été autorisée par la personne concernée[475] et sa finalité, c'est-à-dire, le droit à la portabilité[476], ces deux possibilités renforçant l'exercice du contrôle[477] et la mainmise des personnes concernées sur leurs propres données mises à disposition[478].

160. Afin de gérer leurs données personnelles, les personnes concernées disposent d'un droit à rectification[479] qui permet de modifier, corriger ou encore compléter les informations fournies au responsable de traitement, à travers, si besoin est, d'une déclaration supplémentaire qui rectifie les informations incomplètes ou inexactes. Il est nécessaire de savoir que ce privilège s'accompagne, pour plus de pertinence, d'un droit de suite[480] qui oblige le

---

472 *V. supra §n°110.*

473 RGPD art. 15, *préc.*

474 RGPD consid. 63, *préc.*

475 RGPD art. 15, al. 3, *préc.*

476 RGPD art. 20, *préc.*

477 RGPD consid. 68, *préc.*

478 « *Se trouve ainsi traduite la volonté de renforcer le data subject empowerment, à savoir le pouvoir de contrôle qu'a la personne concernée sur ses données à caractère personnel »,* T. Tombal, M. Ledger, *Le droit à la portabilité dans les textes européens : droits distincts ou mécanisme multi-facettes ?*, R.D.T.I., 2018, n° 72, p. 30.

« *Le nouveau droit à la portabilité des données vise à responsabiliser les personnes concernées au sujet de leurs données à caractère personnel, car il facilite leur capacité à déplacer, à copier ou à transmettre facilement des données à caractère personnel d'un environnement informatique vers un autre »,* Groupe 29, *Lignes directrices relatives au droit à la portabilité des données*, WP 242 rev.01, 5 avril 2017, p. 4.

479 RGPD art. 16, *préc.*

480 RGPD art. 19, *préc.*

responsable de traitement à notifier à chaque destinataire auquel les données ont été communiquées, les rectifications, ajouts ou modifications intervenues[481].

Si les personnes concernées peuvent gérer leurs données lorsque celles-ci sont traitées, une possibilité similaire est accordée quand elles n'ont plus vocation à être utilisées, un tel attribut est conféré par le droit à l'effacement également dénommé droit à l'oubli[482]. Consacré par la Cour de justice de l'Union européenne[483], le droit à l'effacement s'exerce lorsqu'une personne concernée souhaite anéantir tout traitement illicite à son encontre. Ce droit prend du sens, par exemple, en cas de retrait du consentement de la personne concernée, les données personnelles devant être effacées, le traitement n'ayant plus de fondement.

161. Deux derniers pouvoirs, conférés à la personne concernée par l'intermédiaire de son consentement, méritent d'être évoqués, il s'agit d'une part du droit à la limitation[484] et d'autre part du droit d'opposition[485]. Si le premier protège le contenu des données personnelles en autorisant la personne concernée à bloquer l'utilisation de celles-ci qui seront « *verrouillées pendant un certain laps de temps* »[486], le second permet pour la personne concernée de s'élever[487] contre tout traitement de ses propres données, ce qui matérialise une fois de plus l'un des objectifs du règlement européen à savoir le rôle accru de l'individu dans la protection de ses données[488].

---

[481] « *Le droit de rectification comporte donc un double volet, à savoir le droit d'obtenir la correction des données erronées, ainsi que le droit d'exiger que le responsable de traitement « fasse suivre » cette rectification en la notifiant aux destinataires desdites données à caractère personnel, sauf si cela exige des efforts disproportionnés* », T. Tombal, *Les droits de la personne concernée dans le RGPD* in Le Règlement général sur la protection des données (RGPD/GDPR), Larcier, 2018, p. 448.

[482] RGPD art. 17, *préc.*

[483] CJUE, 13 mai 2014, *Google Spain*, aff. C-131/12.

[484] RGPD art. 18, *préc.*

[485] RGPD art. 21, *préc.*

[486] T. Tombal, *Les droits de la personne concernée dans le RGPD* in Le Règlement général sur la protection des données (RGPD/GDPR), *Op cit*, p. 480.

[487] « *Par le biais de ce droit d'opposition, la personne concernée se voit ainsi reconnaitre le droit de remettre en cause cette décision unilatérale du responsable de traitement* », T. Tombal, *Les droits de la personne concernée dans le RGPD* in Le Règlement général sur la protection des données (RGPD/GDPR), *Ibid*, p. 524.

[488] « *Ceci est révélateur d'un autre cheval de bataille du RGPD, à savoir la promotion du droit à l'autodétermination informationnelle de la personne concernée, qui désire comprendre la logique sous-*

162. Dans une logique de protection des données personnelles par les personnes concernées, de nombreux droits s'ajoutent au consentement, lequel est un préalable à tout traitement, afin d'en vérifier l'exact réalisation.

Le consentement est donc, tant en matière contractuelle que pour le domaine des données personnelles, un moteur pour la création d'un contrat ou d'un traitement. Pour ce faire, il est la représentation fidèle de l'expression des parties et personnes concernées.
S'ajoute alors un second rôle pour le consentement, celui d'amener les parties et les personnes concernées vers de nouveaux droits utilisés pour sécuriser au maximum les engagements qui ont été pris.

Si le lien entre consentement au contrat et consentement à l'utilisation de données s'établit par le rôle du consentement, au service pour les parties et les personnes concernées, en ce qu'il traduit leurs volontés et permet à ces dernières d'accéder à de nouvelles prérogatives, ce lien perdure par une autre fonction, le consentement ayant, également, la faculté d'être un remède contre certaines atteintes.

jacente des traitements dont elle fait l'objet », T. Tombal, *Les droits de la personne concernée dans le RGPD* in Le Règlement général sur la protection des données (RGPD/GDPR), *Ibid*, p. 527.

B) Le consentement, remède nécessaire contre les atteintes subies

163. En matière contractuelle, si le consentement est l'élément fondateur du contrat, il dispose également d'une fonction protectrice à l'encontre des atteintes qu'il pourrait subir. Le Code civil fait donc une place non négligeable aux vices du consentement[489] lorsque ce principe est victime d'offense, la finalité de tels actes pouvant entrainer une « *cause de nullité relative du contrat* »[490].

Lorsque de telles situations se présentent, un rapport de force s'établit entre les différents consentements propres aux cocontractants, la partie, plus faible, étant toujours sous l'emprise de l'autre. Il est possible de rencontrer cette hypothèse en matière de données personnelles, preuve que le consentement au contrat et le consentement à l'utilisation de données personnelles sont liés par leurs effets.

En effet, le consentement de la personne concernée n'est pas non plus opaque aux agissements énoncés précédemment. A l'image du cocontractant, envisagé en droit des contrats, le consentement de la personne concernée va, lui aussi, subir des pressions et contraintes. La personne concernée ne sera pas toujours au courant de la réelle finalité de l'utilisation de ses données, sa liberté de consentir se retrouvant tronquée et bafouée. Le plus souvent, la source de désagrément relève du fait que le responsable de traitement use de sa position afin de recueillir le consentement de la personne concernée à l'utilisation de ses données. Un tel conflit ne peut exister que parce que les données personnelles représentent, à l'heure actuelle, une denrée rare[491].

164. Le mécanisme du consentement est donc, à ce titre, pour le règlement européen synonyme d'espoir dans l'objectif de protection des données. Parce qu'il est strictement déterminé, il pourra par ses conditions et effets permettre aux personnes concernées de s'opposer à tout traitement vicié, qui ne respecterait pas la volonté de la personne. A ce sujet, le refus de consentir[492] est donc le moyen

---

489 *V. supra §n°108.*

490 C. civ., art. 1131 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016).*

491 X. Leonetti, *Smartsécurité et Cyberjustice*, Edition PUF, Collection Questions judiciaires, 2021.

492 *V. supra §n°160.*

utilisé pour se protéger des responsables de traitements et des menaces en tout genre, ce qui est le cas notamment en matière de cybercriminalité[493], étant précisé que les personnes concernées ne sont pas encore assez vigilantes[494]. Puisque les données personnelles ne représentent plus seulement une manne d'informations, mais sont également des données monétisables, le risque de commercialisation[495] des données peut être contré par l'utilisation du consentement, seul fondement valable pour le traitement. Ainsi, pour chaque traitement de donnée et tel que cela a déjà été évoqué, en matière médicale ou pour une relation de travail, le consentement permet de faire obstacle.

165. Le consentement est donc pour les données personnelles et les personnes concernées l'arme ultime utilisée afin de se protéger. Ce mécanisme ayant fait ses preuves en droit des contrats, il est fort logique que le règlement général sur la protection des données s'inspire sinon reprenne ses principes. Une nouvelle fois, les consentements soumis à l'étude sont en lien, le consentement au contrat étant l'inspiration du consentement à l'utilisation de la donnée personnelle.

Le lien entre les consentements est certain : il permet dans les domaines respectifs, à savoir le droit des contrats et celui de la donnée personnelle, d'une part d'être au service des parties ou des personnes concernées en faisant respecter leur volonté mais aussi en leur permettant d'accéder à de nouveaux droits pour le faire, d'autre part il permet de s'opposer aux différentes menaces par l'expression d'un refus par exemple. La ressemblance entre ces deux consentements étant, par principe indéniable, il convient de s'y intéresser cette fois d'un point de vue pratique.

493 *V. infra §n°181.*

494 *V. supra §n° 40, 160 et 162 et V. infra §n° 170.*

495 *V. supra §n° 66 et V. infra §n° 174, 214 et 215.*

.

§2 L'existence en pratique du lien entre le consentement à l'utilisation de la donnée personnelle et le consentement au contrat

166. Si le lien entre les deux précédents consentements soumis à l'étude semble, en théorie pour le moins, naturel, il est, également, envisageable que ce soit le cas en fait. En effet, il est désormais question de s'intéresser à la possibilité d'établir un lien entre le consentement classique, qui se rencontre en général en droit des contrats, et le consentement accordé par une personne concernée par l'utilisation de ses données personnelles, d'un point de vue, cette fois, non plus théorique mais purement pratique.

Préalablement aux développements à suivre, concernant l'étude confrontant le consentement à l'utilisation de la « donnée personnelle » et le consentement au contrat, il convient de reprendre les bases de la notion de consentement pour en comprendre les aspects. Pour rappel, *in limine* le consentement s'entend juridiquement comme « *l'acceptation par une partie de la proposition faite par l'autre* »[496]. C'est donc l'échange des consentements qui entraine, inéluctablement, l'accord de volonté qui lie les parties, et qui, par-là, permet la création d'un acte juridique.

167. En consacrant l'article 1109 du Code civil, l'Ordonnance du 10 février 2016[497] s'est efforcée de distinguer les différents contrats en les classant. Ainsi, ce texte énonce que le contrat consensuel est celui qui se « *forme par le seul échange des consentements quel qu'en soit le mode d'expression* »[498]. Le contrat dit consensuel est donc celui qui se crée par le seul accord des volontés, et cela, sans qu'aucun formalisme ne soit imposé. Pour se persuader de l'importance du consentement en lien avec le contrat, il est primordial de se référer, également, à l'article 1172 du Code civil qui énonce une règle, selon laquelle « *Les contrats sont par principe consensuels* »[499].

---

[496] Lexique des termes juridiques, *préc.*

[497] Ordonnance n° 2016-131 du 10 février 2016, *préc*.

[498] C. civ., art. 1109, *préc.*

[499] C. civ., art. 1172, *préc.*

168. Consentir c'est donner un accord à l'ensemble de l'offre contractuelle qui est faite. Consentir est un acte général. Automatiquement quand on consent au contrat, on consent à son contenu puisqu'il n'existe pas de consentement partiel ou parcellaire. Le consentement fait donc le contrat. C'est parce qu'il y a une volonté des parties, qui se traduit par une acceptation, dont la finalité est celle de consentir, que le contrat existe. De ce fait, lorsque les parties au contrat consentent à un contrat qui ne porte pas sur des « données personnelles » ou lorsque les parties au contrat consentent à un contrat qui, *a contrario*, porte sur des « données personnelles », c'est en réalité le même type d'acceptation qui est donnée.
Pour le dire autrement, dans la précision précédente, peu importe sur quoi il porte, le consentement est le même, il a donc la même portée. Consentir c'est donc consentir, et ce, qu'il y ait la présence, ou pas, de « donnée personnelle ».

La question du consentement à l'utilisation des données est automatiquement en lien avec celle du consentement au contrat. Consentir à l'utilisation des données personnelles relève d'un accord qui est donné au sein d'un contrat. Certes, il ne s'agit pas forcément dans cette hypothèse de consentir à un acte juridique contractuel mais bien à consentir, à l'intérieur de ce contrat, à ce que les données qui y sont contenues, directement ou indirectement, soient utilisées[500]. A ce titre, il y a donc un lien entre le fait de consentir à l'utilisation de la « donnée personnelle » et le consentement au contrat.

169. Si un lien existe entre ces deux notions, le Code civil et l'Ordonnance se sont pour autant attachés d'apporter quelques précisions, en guise de mise en garde pour tout ce qui est lié à la notion d'information. En effet, puisque les « données personnelles » représentent des informations intimes, au caractère sensible, la réforme du droit des contrats a consacré l'obligation d'information, qui s'applique pleinement pour les « données personnelles ». Aussi, l'article 1112-1 du Code civil[501] impose certaines conditions aux parties, comme celles d'informer ou d'avertir de l'existence d'éléments spécifiques dans le contrat lorsque ce dernier repose sur l'utilisation de « données personnelles ».

---

[500] M. Bourgeois, « *Droit de la donnée* », *Op cit.*

[501] C. civ., art. 1112-1 (*Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016*).

170. L'idée qui domine l'étude du consentement dans le contrat en lien avec la « donnée personnelle », est l'idée que consentir au contrat signifie automatiquement consentir à ce que des données soient récoltées, voir utilisées, au sein de ce contrat. Il y a donc un lien entre le consentement au contrat, lui-même, et le consentement donné à l'utilisation de la « donnée personnelle ».

La notion de consentement étant précisée, il convient de s'intéresser, de manière concrète, au lien qui existe entre ces deux consentements et ainsi justifier cette connexion. S'il a été énoncé que consentement au contrat et consentement à l'utilisation de la donnée personnelle étaient plus ou moins synonymes, il convient de le prouver par des exemples factuels. Pour ce faire, deux idées se dégagent. La première situation démontre que le consentement à l'utilisation des données personnelles intervient pour le consentement à un contrat, quel qu'il soit. La seconde situation recouvre l'idée que le consentement à l'utilisation des données personnelles découle, justement, du consentement à ce contrat. Pour le dire simplement, ces deux consentements sont, chacun à leur tour, au service de l'autre.

171. En pratique, comment se caractérise ce lien ? Dans quelle mesure le consentement à l'utilisation de la donnée vient-il s'inscrire avec le consentement au contrat ?

Lorsqu'une personne concernée navigue sur internet et souhaite par exemple, cas de figure récurrent, faire des achats, quels qu'ils soient, l'interaction entre ces deux consentements prend tout son sens[502]. En effet, à travers les outils informatiques, lorsqu'un produit intéresse un utilisateur, un acheteur, il se rend sur un site web. Immédiatement le site en question va proposer à l'utilisateur d'accepter ou non à un suivi. Déjà, sans parcourir « physiquement » le site, un consentement est demandé concernant l'acceptation de suivi. En général la personne accepte sans s'attarder sur la démarche. Dans certains cas, il peut lui être demandé de gérer ce suivi, sachant que cette procédure est éminemment plus

[502] P. Le Tourneau, *Chapitre 411 : Contrat de commerce en ligne : données de fait,* in *Contrats du numérique,* éd., Dalloz référence, 2021-2022.

fastidieuse que d'accepter purement et simplement. Il ne faut pas oublier que l'utilisateur, dans l'exemple d'espèce, cherche à acquérir un produit. Il souhaite faire cela le plus rapidement possible, aussi, c'est pourquoi il acceptera à cette première demande, sans s'y intéresser.

Voilà un cas de figure qui démontre que l'utilisateur qui, pourtant, cherchait à se procurer un produit se retrouve à devoir consentir à un suivi de ses données[503]. D'un côté, ce premier consentement rend service à l'individu puisque le site internet fait cela dans son intérêt et dans celui de son client pour plus de confort. La personne sera reconnue sur le site internet ce qui peut faciliter une recherche future, mais la personne sera surtout sollicitée, ce qui peut représenter l'avantage d'être au courant des nouveaux produits présentés par la marque en question. De l'autre, le client s'oblige à accepter ce suivi alors qu'il ne le voudrait peut-être pas.

De plus, lorsque l'utilisateur aura choisi le produit qui l'intéresse, il devra pour l'acheter créer un compte, encore une fois dans un souci de traçabilité du client, de marketing, mais aussi pour qu'il renseigne ses informations personnelles afin que son achat puisse lui être destiné. A ce titre, la personne concernée consentira à donner son prénom, nom, date de naissance, adresse, numéro de téléphone, email etc.…

Si ces informations sont utiles, pour autant, elles représentent un atout pour la marque, en tant que responsable de traitement, qui pourra les réutiliser afin de solliciter l'acheteur, ou pire encore, afin d'échanger, vendre, transmettre, ces données à des partenaires, c'est-à-dire, d'autres responsables de traitement, lesquels solliciteront à leur tour l'acheteur alors qu'il n'a rien demandé en ce sens.

L'utilisateur qui souhaitait acheter un produit se retrouve dans la peau d'une personne concernée ayant obligation de transmettre ses propres données personnelles pour ce faire. Sans s'en rendre compte l'utilisateur aura consenti sciemment à ce que le responsable de traitement capte et utilise par la suite ses données. Si le Règlement européen se veut protecteur des utilisateurs et personnes

[503] C. Féral-Schuhl, *Section 1 – Définitions – 122.11. Un outil multiforme,* in *Livre 1 : Les données à caractères personnels*, Praxis Cyberdroit, 2020-2021.

concernées, en pratique la réalité est tout autre puisque c'est bien le responsable de traitement qui bénéficie d'une position dominante[504].

Le lien entre consentement au contrat et consentement à l'utilisation des données personnelles est donc indéniable. Ils ne font qu'un. A l'inverse, le lien est, une fois encore, perceptible puisqu'une personne qui ne coopérera pas et ne transmettra pas ses données personnelles ne pourra pas se rendre sur certains sites et ne pourra pas acheter tel ou tel produit. Le consentement à l'utilisation des données et le consentement au contrat sont donc complices et complémentaires. L'un ne fonctionne pas sans l'autre et inversement.

Le second point qui met en lumière la similitude entre ces deux consentements relève d'un constat simple, à savoir que les stipulations propres à la protection des données personnelles sont toujours insérées dans le contrat ou dans les conditions générales de vente de celui-ci[505]. En pratique, cela veut dire qu'il n'y a pas de stipulations spécifiques concernant la mise à disposition des données personnelles. Le consentement à l'utilisation des données personnelles fait donc partie d'un consentement global, c'est-à-dire le consentement au contrat initial.

En réalité, le fait de se rendre sur un site internet, le fait d'acheter ou de vendre un produit, le fait d'accepter un service oblige à consentir à l'utilisation de ses données et ces deux phénomènes se retrouvent donc au même plan. Consentir à un contrat, c'est consentir à l'utilisation de ses données personnelles. Avec le développement toujours croissant d'internet, la société étant de plus en plus informatisée, ce constat n'est pas près de s'arrêter.

---

504 « *Certes, à travers les dispositions du règlement, les personnes concernées voient des limites mises à l'utilisation de leurs données et peuvent réclamer qu'une prévalence soit accordée à leurs intérêts par rapport à ceux du responsable du traitement mais toute pesée d'intérêt exige qu'un critère soit fixé pour opérer cette pesée. Prenons un exemple tiré d'une expérience récente : une compagnie d'assurance me propose une réduction importante de mes primes d'assurance auto, à condition que j'accepte l'installation d'un mouchard dans ma voiture (…), l'enregistrement de telles données est-il compatible avec la conception traditionnelle défendue par le droit de l'assurance ?* », T. Tombal, *Les droits de la personne concernée dans le RGPD* in Le Règlement général sur la protection des données (RGPD/GDPR), *Op cit*, p. 18.

505 C. Féral-Schuhl, *Section 7 – Droit d'opposition (RGPD, art. 21) – 112.123. Mise en œuvre du droit d'opposition,* in *Livre 1 : Les données à caractères personnels*, *Op cit*.

172. Pour synthétiser l'analyse précédente, qu'il s'agisse d'effets positifs ou négatifs, les consentements, tant au service de l'utilisation des données que concédés pour un contrat, ont, par nature, mais également en pratique, beaucoup de similarité.

En effet, l'acceptation au contrat est identique, que celui-ci attrait directement avec les données personnelles ou que ce lien ne soit pas si proche. De fait, lorsqu'une partie, une personne concernée, consent à un contrat, c'est, en réalité, à la globalité du contrat qu'elle consent. Toutefois, puisque la donnée personnelle présente une certaine dangerosité quant à l'utilisation qui peut en être faite et face aux éventuelles atteintes qu'elle peut porter aux libertés individuelles, elle est donc naturellement soumise, dans son utilisation spécifique, à un consentement spécifique.

Section 2 : Le consentement à l'utilisation de la donnée personnelle est distinct du consentement au contrat

173. Le consentement à l'utilisation de la donnée personnelle est particulier, d'une part en ce qu'il déroge avec le consentement traditionnel en se distinguant du consentement au contrat (Paragraphe 1) et d'autre part à cause des modalités qui lui sont applicables (Paragraphe 2).

§1 Le principe de la distinction

174. Dans l'esprit d'atténuer les propos développés ci-dessus, voici les raisons d'une distinction entre consentement à l'utilisation des « données personnelles » et consentement au contrat. Si le droit civil français traite du consentement, quel qu'il soit, en son entier, le droit relatif aux données personnelles ne s'aligne pas sur cette réflexion. En effet, ce dernier, au travers du règlement européen, semble promouvoir l'idée d'une distinction, laquelle existerait entre le consentement propre à l'utilisation des « données personnelles », d'une part, et le consentement au contrat, d'autre part.

C'est dans cet esprit qu'il convient d'analyser le principe de la distinction entre ces deux consentements en se posant la question de savoir si la protection accordée à la personne concernée est seule responsable (A) ou s'il existe d'autres critères (B) ?

A) La protection accordée aux personnes concernées, seule responsable de la distinction ?

175. Pour traiter du consentement à l'utilisation des « données personnelles » et comprendre les rouages de celui-ci, il convient de se demander pourquoi et à qui ce consentement est-il donné ? La réponse émane du règlement général sur la protection des données personnelles dont l'objectif est de rééquilibrer le contraste entre les utilisateurs quelconques et les géants de l'informatiques que sont les serveurs et plateformes numériques ou encore les réseaux sociaux. En effet, le constat est le suivant, à savoir que les utilisateurs n'ont, de nos jours, plus la

lucidité pour se protéger eux même des géants de l'informatique qui ne se privent pas pour récolter et utiliser toutes ces « données personnelles » (à des fins lucratives et commerciales) et cela, sans jamais en informer leurs utilisateurs, n'y recueillir leurs consentements ![506]

Quotidiennement, une multitude d'informations, intimes, sont partagées par les utilisateurs sur les réseaux sociaux, par exemple sur Facebook, Snapchat, Instagram ou encore sur Twitter. Ainsi, les « données personnelles » étant devenues de réelles « *ressources économiques* », il convient de redonner une place centrale au consentement, dans le but d'éviter toutes dérives qualifiées de « *commercialisation des données personnelles* »[507].

Cette démarche, à l'ère du règlement général sur la protection des données, conduit en effet à faire prendre conscience aux utilisateurs, ainsi qu'aux responsables de traitements, que la distinction entre consentement au contrat et consentement à l'utilisation des « données personnelles » existe et elle doit s'appliquer. Si ce travail parait essentiel, l'accomplissement de celui-ci n'est pas pour autant aisé. La notion de consentement, tel qu'elle est éclairée par le règlement sur la protection des « données personnelles » décèle une position aux apparences ambigües. En effet, si l'utilité première du consentement est celle de protéger les personnes, une nature plus déplaisante semble pouvoir lui être attribuée, celle d'ouvrir des possibilités aux responsables de traitements.

176. Pour dépeindre le « rôle ambigu » du consentement, quelques auteurs estiment qu'il a favorablement « *un rôle plutôt protecteur, c'est le cas quand il sert de fondement au traitement* », mais prétendent néanmoins, « *qu'en revanche, il peut aussi être un élément sur lequel le responsable de traitement va déroger à des interdictions posées par le texte* »[508].

---

[506] « *Le point de départ, c'est que nous, internautes, sommes tous désemparés face aux GAFA (Google, Apple, Facebook et Amazon). Nous nous en servons quotidiennement, mais nous n'avons aucun moyen de dire non au pillage des données* », URL : https://www.capital.fr/economie-politique/et-si-demain-vous-vendiez-vos-donnees-personnelles-a-facebook-1268001

[507] J-F. Kerleo, *La transparence en droit*, thèse de doctorat en droit Public, Lyon lll, octobre 2012 (extrait, sans note de bas de page).

[508] A. Debet, *Le consentement dans le RGPD : rôle et définition*, (extraits, sans note de bas de page).

Consentir à l'utilisation de ses « données personnelles » serait donc risqué pour les utilisateurs. Effectivement, grâce à l'accord de ces personnes, les responsables de traitements des données sensibles vont pouvoir utiliser celles-ci et cela pour un but parfois contraire pour lesquelles elles ont été collectées.

177. Le consentement représente alors un des prémices obligatoires à l'utilisation de « données personnelles » et la responsabilité des responsables de traitement en est la finalité. Par-là, le règlement général semble faire supporter au consentement quelque chose qu'il ne maitrise pas, puisque ce sont les responsables qui doivent prouver que le consentement a été proposé et requis. Énoncer l'inverse viendrait à sanctionner l'utilisateur d'avoir volontairement donné, sans prendre garde, son consentement, alors que c'est pourtant le responsable de traitement qui utilise à des fins malveillantes ses « données personnelles ».

De consentement au contrat à consentement pour l'utilisation des « données personnelles », la notion est des plus importantes puisqu'elle montre aux personnes concernées, tant utilisateurs que responsable de traitements, les enjeux qui s'y affèrent.

B) Le formalisme et la portée des consentements, autres critères de la distinction

178. Il convient, dès maintenant de s'intéresser plus frontalement aux différences entre les deux formes de consentement. Pour étayer cette démonstration, il est nécessaire d'analyser l'article « *Capacité et consentement au contrat de données à caractère personnel et au contrat* »[509].En effet, selon l'auteure, tant du point de vue du fond, que de la forme, les consentements énoncés précédemment diffèrent. Il sera donc, d'abord, question d'étudier les divergences liées au formalise des consentements, afin de s'intéresser, ensuite, aux disparités attachées au fond des consentements, c'est-à-dire s'intéresser, en pratique, à leur portée.

179. L'idée la plus perceptible, pour départager ces deux types de consentements, concerne le formalisme.

Si classiquement en droit des contrats l'acte contractuel est un échange de volontés, un accord entre deux ou plusieurs personnes, le consentement au traitement de données à caractère personnel n'émane que d'une seule volonté. Cela est possible puisque les données personnelles n'appartiennent, fort heureusement, qu'à une seule et même personne, laquelle est libre de choisir ce qu'il adviendra, ce qu'il sera fait, ou non, de ses données intimes[510].

Ce postulat étant posé, il ne faut, pourtant, pas arrêter la distinction, entre ces deux types de consentement, seulement sur le nombre de volontés[511]. Cette atténuation appelle deux précisions. D'une part, si l'unique volonté propre au consentement

---

[509] F. Rogue, *Capacité et consentement au traitement de données à caractère personnel et au contrat*, AJ Contrat 2019, p. 370.

[510] « *Le consentement au traitement semble de prime abord être bien distinct du consentement contractuel. Il émane d'une seule personne, la personne concernée, dont les données à caractère personnel sont susceptibles de faire l'objet. En droit des contrats, au contraire, il ne peut y avoir une volonté unique à l'origine de la création d'un contrat. Ce qui fait l'essence de l'acte contractuel, c'est l'accord de volonté* », F. Rogue, *Capacité et consentement au traitement de données à caractère personnel et au contrat*, *Ibid*.

[511] « *En droit des obligations des manifestations de volonté, unilatérales, qui emportent des effets juridiques. Ainsi ce n'est pas tant le nombre de volontés exprimées qui distingue le consentement au traitement du consentement contractuel* », F. Rogue, *Capacité et consentement au traitement de données à caractère personnel et au contrat*, *Ibid*.

au traitement de données personnelles est un facteur utile pour le distinguer du consentement au contrat, la distinction, n'existe pas, uniquement, par rapport à cela. D'autre part, l'autre constat consiste à souligner l'importance des informations utiles au traitement des données personnelles, puisque cette volonté unique renforce l'utilisation d'informations personnelles, intimes, propres à la personne concernée. Ce consentement est, de ce fait, inégalable puisque les données sont, comme leur nom l'indique, personnelles.

180. L'autre réflexion, sur cette analyse, concerne la portée même du consentement au traitement des données personnelles.

Tout d'abord, il serait possible d'accorder au consentement une « *fonction de légitimation du traitement* »[512]. Cette fonction réfère, d'une part, à un acte plutôt noble, qui est le fait de légitimer, en l'occurrence légitimer le traitement des données personnelles. Pour autant, elle peut être assimilée, également, à une opération ayant moins de prestige, lorsqu'elle est utilisée comme « *base légale ''par défaut'', c'est-à-dire celle à laquelle se référer si l'on n'arrive pas à démontrer que le traitement est nécessaire* »[513], ce qui correspond en pratique à utiliser ce mécanisme lorsqu'aucune des cinq autres bases légales ne fonctionne réellement.

Plus encore de savoir si l'adjectif de légitimation attribué au consentement est honorable ou, au contraire, méprisable, cette qualité contribue, malgré elle, à la distinction. En effet, en droit des obligations, le consentement créé le contrat, alors qu'en matière de traitement de données, il est possible d'outrepasser, celui-ci, si d'autres bases légales s'imposent[514]. Puisque le consentement au traitement a deux fonctions, d'une part celle consentir et d'autre part celle de légitimer, il ne représente pas l'âme du traitement alors que le consentement est l'essence du contrat.

---

[512] A. Debet, *Le consentement dans le RGPD : rôle et définition*, *Op cit.*

[513] F. Rogue, *Capacité et consentement au traitement de données à caractère personnel et au contrat*, *Op cit*, p. 370.

[514] « *S'agissant du consentement au contrat, celui-ci est l'essence même du contrat*, , *le consentement est indispensable à la création d'un contrat alors qu'il ne l'est pas pour la création d'un traitement de données à caractère personnel »,* F. Rogue, *Capacité et consentement au traitement de données à caractère personnel et au contrat*, *Ibid.*

181. L'ultime différence complétant l'analyse, développée en amont, s'apprécie au travers du concept d'autodétermination[515], principe fondé par le critère des données personnelles, informations intimes, fragiles et privées et le rôle conféré, à ce propos, aux personnes concernées[516].

Ce principe, dégagé par la Cour constitutionnelle fédérale allemande de Karlsruhe[517], crée « *un droit pour chaque individu de décider lui-même de la communication et de l'emploi des informations le concernant* »[518]. Actuellement, depuis le 1er juin 2019, il s'applique toujours et constitue, l'alinéa 2 de l'article 1er[519] de la loi « Informatique et Libertés », nouvellement rédigée[520]. Par ailleurs, il s'inscrit, pleinement, dans l'idéal et la logique fondatrice du règlement européen, à savoir, de donner, pour les personnes concernées, une conscience, ainsi qu'un rôle à jouer dans l'enjeu de protection de leurs propres données[521].

Toutes ces constatations démontrent, une fois encore, sans aller jusqu'à évoquer le terme de fracture, qu'il existe une réelle disparité entre le consentement au contrat et le consentement au traitement des données personnelles. De par la sensibilité de l'objet du contrat relatif au traitement de données à caractère

---

515 « *Le consentement au traitement est caractéristique d'un droit de la personne concernée à l'auto-détermination s'agissant de l'utilisation de ses données personnelles* », N. Martial-Braz, *Le renforcement des droits de la personne concernée*, Dalloz IP/IT 2017, p. 253.

516 « *S'agissant d'un élément de sa vie privée, on comprend bien cette volonté de conférer à la personne un plus grand contrôle* », F. Rogue, *Capacité et consentement au traitement de données à caractère personnel et au contrat*, *Op cit*.

517 Cour constitutionnelle fédérale, 16 février 1983, *BVerfGE*, tome 62, p. 1 ; Analyse Fromont, *RD publ.* 1983, p. 954.

518 URL : https://www.senat.fr/lc/lc62/lc621.html

519 « *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* », Art. 1er, al. 2, Loi n°78-17 du 6 janvier 1978, Loi relative à l'informatique, aux fichiers et aux libertés, version en vigueur depuis le 17 juin 2019.

520 « *Le droit à l'autodétermination informationnelle (...) renforce positivement les principes énoncés à l'article 1er de la loi Informatique et Libertés en affirmant la nécessaire maitrise de l'individu sur ses données* », URL : https://www.cnil.fr/fr/ce-que-change-la-loi-pour-une-republique-numerique-pour-la-protection-des-donnees-personnelles

521 « *En instaurant une nouvelle conception du rapport à la personne avec ses données, chaque individu se voit reconnaitre une certaine autonomie dans la gestion de ses données personnelles* », J. Rochfeld, *Données personnelles : quels nouveaux droits ?*, Actualité, Statistique et société, Vol. 5, n°1, avril 2017, p. 47.

personnel, le consentement, relatif à ce dernier, « *se rapproche beaucoup plus du consentement donné en matière médicale* »[522].

En effet, la problématique d'autodétermination informationnelle des données est sensiblement la même en ce qui concerne le domaine des données personnelles et celui du droit médical. Pour ce qu'elles représentent, les atteintes et les enjeux, autour de la question des données personnelles et plus particulièrement aux données de santé est important, ne cessent de s'intensifier, ce qui conduit, de ce fait, à renforcer le principe d'autodétermination.

182. Si en soi, la collecte, le partage, la révélation minimaliste de donnée personnelle ne représente pas véritablement de danger pour un individu, c'est en revanche, le regroupement de l'ensemble de ces données qui cause des difficultés[523].

Malheureusement, cette tendance ne semble pas en déclin, bien au contraire, puisque les informations individuelles ont vocation à devenir *« de plus en plus collectives* »[524]. Aussi, pour éviter un « *capitalisme sauvage* » des données personnelles, certains auteurs proposaient une « *protection sociale* » de celles-ci, alternative complémentaire à l'autodétermination informationnelle, pour renforcer les barrières à leur circulation sans contrôle[525]. Malgré ces bonnes

---

[522] F. Rogue, *Capacité et consentement au traitement de données à caractère personnel et au contrat*, *Op cit*, p. 370.

[523] « *Les mégadonnées de santé couvrent l'ensemble des données sociodémographiques et de santé disponible auprès des différentes sources qui les collectent, pour des raisons très diverses. Les données de santé ne sont en effet plus seulement collectées par des entités organisées (administrations, entreprises, associations) mais aussi mise en ligne par les individus eux-mêmes ou par des tiers, ou recueillies de manière automatique. Elles ne correspondent plus seulement aux caractéristiques objectives de l'individu (âge, sexe, profession, pathologies) ; il peut s'agir d'informations sur ses habitudes alimentaires, son sommeil, ses relations, ses déplacements ou sa sédentarité, ou encore de signaux biologiques ou corporels. Disséminées, ces informations disent peu sur les individus et leur santé. Mais la dynamique de l'économie numérique pousse à leur regroupement. Ainsi moteurs de recherche et réseaux sociaux sont-ils dépositaires de pans entiers de notre vie privée. La publicité joue un grand rôle dans ce regroupement : plus le profil est précis, plus les publicités adressées seront potentiellement pertinentes* »[523], E. Debiès, *Big data de santé et autodétermination informationnelle : quelle articulation possible pour une innovation protectrice des données personnelles ?*, Revue française d'administration publique, vol. 167, no. 3, 2018, pp. 565-574.

[524] T. Bizet, *L'ambition individualiste de l'autodétermination informationnelle*, International Journal of Digital and Data Law, Vol 3, 2017, p. 54.

[525] A. Fluckiger, *L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?*, Pratique juridique actuelle, 2013, vol. 22, n° 6, p. 837-864.

volontés, d'autres en revanche, n'osent dissimuler un sentiment fataliste et résigné, accusant la société moderne d'être responsable des maux causés aux individus et à leurs données personnelles[526].

L'émoi partagé, précédemment, rejoint l'opinion, déjà révélée, quelques années auparavant, à propos de l'absence de contrôle des individus sur leurs propres données[527]. Il faut espérer, pour le bien des individus, de leurs données personnelles et de la société, en général, que ces différents aveux n'aient plus la même virulence, le règlement général sur la protection des données accordant, à nouveau, à l'individu la maitrise de ses données personnelles.

183. Il ne serait pas raisonnable de se convaincre que la distinction de représentation des consentements, précédemment évoqués, n'existe que du fait de la sensibilité, ou non, de l'objet des contrats. Si le consentement utilisé en droit des données personnelles s'accorde avec celui pratiqué par le domaine médical, notamment parce que les contrats s'y afférent constituent une intrusion pour l'intimité des personnes concernées (acte pratiqué touchant à la vie privée, informations intimes collectées et utilisées), ce critère n'est, pour autant, pas péremptoire. En effet, nombreux sont les contrats, dits classiques, tels que, par exemple, le contrat de vente, dont l'objet principal repose sur des valeurs importantes.

Pour autant, même si d'autres contrats que le contrat médical[528] ou celui relatif au traitement de données personnelles[529] reposent sur des éléments et objets rares ou

---

526 « *Dans un univers de plus en plus technologique, règne de la transparence maximale, il est illusoire d'imaginer que l'on puisse véritablement décider si et dans quelle mesure une information nous concernant peut-être diffusée et à autrui, détruite ou oubliée* », E. Debiès, *Big data de santé et autodétermination informationnelle : quelle articulation possible pour une innovation protectrice des données personnelles ?*, *Op cit*, pp. 565-574.

527 « *Les développements technologiques de ces dernières années ainsi que les pratiques sociales qu'ils génèrent semblent battre en brèche la capacité, voir même la volonté, des individus d'exercer un véritable contrôle sur leurs données personnelles* », C. Lazaro et D. Le Métayer, *Le consentement au traitement des données personnelles : une perspective comparative sur l'autonomie du sujet*, Revue juridique Themis, 43 (3), 768-815, 2015.

528 *V. supra §n°138.*

529 *V. supra §n°165.*

onéreux, les deux derniers contrats précités ont, par essence, un caractère intrusif et indiscret dans le rapport, qu'ils exercent, aux personnes concernées.

184. La distinction étant admise, il convient dès à présent de s'intéresser aux différentes conditions relatives au consentement lorsque celui-ci repose sur l'utilisation des « données personnelles ».

§2 Les modalités du consentement à l'utilisation des données personnelles

185. Le règlement général sur la protection des données prône un certain type de consentement, à savoir celui par lequel la personne concernée adhèrera, en toute connaissance de cause, à l'utilisation de ses « données personnelles »[530]. Aussi, plusieurs interrogations sont à soulever concernant les modalités du consentement lorsque celui-ci porte sur l'utilisation de celles-ci. Pour obtenir un consentement licite et conforme au règlement européen, il faut, en effet, se demander qui a la capacité de consentir et sous quelles formes doit-il être requis ?

186. Avant d'étudier les règles relatives à la capacité du consentement et au formalisme de celui-ci, lorsqu'il porte sur l'utilisation des « données personnelles », il convient de s'intéresser sur ces mêmes exigences tel que prévu par le droit commun français, à savoir le droit civil. Le Code civil attend d'une personne dite « capable » qu'elle ait au moins la majorité, en ce sens, l'article 414 indique que « *La majorité est fixé à dix-huit ans accomplis ; à cet âge, chacun est capable d'exercer les droits dont il a la jouissance* »[531]. Pour trouver une condition propre à l'existence du consentement, il faut se référer également à l'article 1129 du Code civil qui dispose que « *Conformément à l'article 414-1, il faut être sain d'esprit pour consentir valablement à un contrat* »[532].

Le droit commun français caractérise donc une personne capable de consentir comme une personne qui est saine d'esprit et qui a la majorité, c'est-à-dire au moins 18 ans.

187. Mais alors, qui peut véritablement consentir lorsque cette volonté est employée pour l'utilisation des « données personnelles » ? En son article 1er, le règlement général sur la protection des données décrit son objet et ses objectifs et instaure le fait que « *Le présent règlement établit des règles relatives à la*

---

[530] RGPD art. 4, al. 11, *préc.*

[531] C. civ., art. 414 *(L. nº 2007-308 du 5 mars 2007, en vigueur le 1er janv. 2009).*

[532] C. civ., art. 1129, *préc.*

protection des personnes physiques à l'égard du traitement des données à caractère personnel »[533].

L'article 7 de ce même règlement, qui traite des conditions applicables au consentement, ne fait pas plus référence à l'âge requis pour consentir valablement. Cependant, il précise que les personnes qui pourront consentir à l'utilisation de leurs « données personnelles », seront des personnes physiques, en énonçant toutefois, qu'il *« ne s'applique pas aux données à caractère personnel des personnes décédées* »[534], ce qui exclut de ce fait les personnes morales, sans pour autant imposer, à ce moment-là, une quelconque condition relative à l'âge.

Toutefois, le règlement général sur la protection des données accorde une place particulière à certaines personnes physiques, notamment du fait de leur certaine fragilité, « *Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel* »[535].

188. Il faut, alors, attendre l'article 8 de ce même règlement, relatif aux conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information, pour y trouver un curseur, fixant l'âge des personnes capables de consentir à l'utilisation de leurs « données personnelles ». Celui-ci énonce, à ce titre, une première condition en disposant que « *le traitement des données à caractère personnel relatif à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans* ». Ce principe trouve, pour autant, une atténuation puisque « *Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure ou, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant* »[536].

Ainsi, contrairement au droit commun français, pour le règlement, une personne à, licitement, la capacité de consentir des lors qu'elle est âgée d'au moins 16 ans, là où l'article 414 du Code civil impose la majorité.

---

[533] RGPD art. 1er, *préc.*

[534] RGPD consid. 27, *préc.*

[535] RGPD consid. 38, *préc.*

[536] RGPD art. 8, *préc.*

Une éventualité est toutefois accordée aux États membres qui *« peuvent prévoir par la loi un âge inférieur, (…), pour autant que cet âge inférieur ne soit pas en dessous de 13 ans* »[537].

Si cette faculté existe, il faut souligner qu'elle n'a pas été utilisée en France. En effet, il ressort de l'article 20 de la loi 20 juin 2018, que les députés ont voté l'âge de la majorité numérique à 15 ans, dès lors, « *un mineur peut consentir seul à un traitement de données à caractère personnel en ce qui concerne l'offre directe de services de la société de l'information à compter de l'âge de quinze ans* »[538].

Cela montre que la France s'est positionnée sur un encadrement plus souple que ce qui aurait pu être énoncé, sans toutefois aller jusqu'à la limite de l'âge de 13 ans.

189. Les conditions de capacité et de l'âge requis pour consentir étant posées, il convient, toutefois, de regretter la mention relative à l'obligation faite au responsable de traitement qui « *s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles* »[539].

En effet, ces propos, visant à crédibiliser la responsabilité des responsables de traitements, ne peuvent être, valablement, accueilli, tant la phase de vérification à distance, sans moyens intrusifs, semble impossible. D'ailleurs, à cet occasion, une consultation orchestrée par la Commission nationale de l'informatique et des libertés dénonçait le fait que, « *Ces principes posés, les textes ne précisent pas : les modalités de vérification de l'âge et de recueil du consentement* »[540].

En pratique, comment s'assurer, qui plus est à distance, que l'enfant n'a pas lui-même consenti, mais qu'il a bien été accompagné, pour ce faire, par son parent ou son tuteur responsable ?

---

[537] RGPD art. 8, *préc.*

[538] Art. 20, Loi n° 2018-493 du 20 juin 2018, *préc.*

[539] RGPD art. 8, *préc.*

[540] N. Maximin, *La CNIL consulte sur les droits numériques des mineurs*, Dalloz actualité, 04 mai 2020.

L'article 8, précité, énonce une phase de contrôle et de vérification réalisée par le biais de « *moyens technologiques disponibles* », permettant de justifier que celle-ci est sécurisée. Pour autant, en réalité, la solution technologique ne permet pas plus de solutions qu'elle ne pose de problèmes.

190. La question de la vérification de l'âge des utilisateurs d'internet est cruciale. Si l'enjeu des données personnelles se confronte, particulièrement, aux utilisateurs adultes, il ne faut pas oublier les sujets plus fragiles que sont les enfants.

De par leur caractère naturellement innocent et candide, ces derniers sont naïfs et ne se rendent pas compte des dangers que représente internet. Pourtant les risques, aussi divers que variés, existent : *contenus non adaptés, écran et santé, mauvaises rencontres en ligne, cyber-harcèlement, propagande, usurpation d'identité, etc…*[541]

Aussi, il semble pertinent d'évoquer un problème, en particulier, en rapport avec la thématique de la vérification de l'âge sur internet. Le phénomène de l'accès des personnes mineur à la pornographie est, en effet, en plein essor et directement en lien avec l'exposition des données personnelles[542].

De nombreuses enquêtes prouvent que la jeune génération[543] est, de plus en plus, confrontée à la pornographie, et cela de plus en plus jeune[544]. Cette exposition, sans aucune méfiance, concerne, par la même occasion, toutes formes de contenus inappropriés et choquants.

Alors, il est urgent de se demander comment éviter un tel fléau ? Existe-t-il des solutions au problème de la vérification de l'âge sur internet afin de protéger les

---

[541] URL : https://www.e-enfance.org/les-risques-sur-internet

[542] « *La pornographie est facilement accessible, les jeunes n'ont aucune difficulté à la trouver. L'accès des jeunes à la pornographie est un fléau contre lequel on doit lutter* », S. Comblez, *Rapport annuel e-Enfance*, 2019, p.16.

[543] « *Génération YouPorn* » en référence au nom de l'un des sites web à caractère pornographique, F. Kraus, *Génération YouPorn : mythe ou réalité ? Enquête sur l'influence des nouvelles technologies sur les comportements sexuels des jeunes*, Enquête de l'Ifop pour CAM4.fr auprès des jeunes âgés de 15 à 24 ans, Octobre 2013.

[544] « *Un tiers des 18-30 ans a déjà été exposé à du porno à l'âge de 12 ans* », Étude OpinionWay pour 20 Minutes administrée en ligne entre le 03 et le 04 avril, 1179 répondants représentatifs des 18-30 ans en France selon la méthode des quotas – Vague 51.

enfants, tant contre les contenus choquants et inappropriés (pornographies, violences en tout genre) que sur l'utilisation de leurs données personnelles ?

Preuve que ce combat n'est pas négligé, bien au contraire, le Président de la République française, lui-même, à l'occasion d'un discours a tenu a rappelé que la protection de l'enfant était une priorité[545].

L'engagement pris par le chef de l'État lors du discours, prononcé à l'Unesco, n'est pas resté vain. En effet, conscient que la portée de l'article 227-24 du Code pénal[546] était faible, pour ne pas dire inexistante en matière de numérique et pour remédier à cela, un amendement a été adopté, le 10 juin 2020, par le Sénat[547], afin « *d'instituer une nouvelle procédure destinée à obliger les éditeurs de ces sites pornographiques à mettre en place un contrôle de l'âge de leurs clients* »[548]. Cette procédure se réalise, notamment, à travers ce que propose l'article 22 de la loi 30 juillet 2020[549], à savoir l'instauration d'un nouvel alinéa complétant ainsi l'article 227-24 du Code pénal comme suit « *Les infractions prévues au présent article sont constituées y compris si l'accès d'un mineur aux messages mentionnés au premier alinéa résulté d'une simple déclaration de celui-ci indiquant qu'il est âgé d'au moins dix-huit ans* »[550].

---

[545] « *Et puis, le troisième sujet sur lequel je voulais m'exprimer devant vous. Vous dire notre mobilisation, mon engagement, c'est aussi la protection des enfants dans l'espace numérique. C'est une priorité qui est très importante. C'est protéger nos enfants face à de nouvelles menaces, de nouvelles transformations. Il y a 30 ans, le numérique n'était pas ce qu'il était aujourd'hui* », Discours du Président Emmanuel Macron pour le 30e anniversaire de la Convention internationale des droits de l'enfant, 20 novembre 2019.

[546] « *Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent, incitant au terrorisme, pornographique ou de nature à porter gravement atteinte à la dignité humaine ou à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75 000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur. Lorsque les infractions prévues au présent article sont soumises par la voie de la presse écrite ou audiovisuelle ou de la communication au public en ligne, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables* », C. pén., art. 227-24, *préc.*

[547] Amendement n°92 rectifié au texte n° 20192020-483, Après l'article 11 (Adopté), Protection des victimes de violences conjugales, M. Mercier.

[548] URL : https://www.senat.fr/amendements/2019-2020/483/Amdt_92.html

[549] Loi n°2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales (1).

[550] C. pén., art. 227-24 al. 3 (*Modifié par Loi n°2020-936 du 30 juillet 2020 – art. 22*).

191. Bien plus que sur la simple utilisation du numérique par les jeunes, ce qui en soit ne pose pas de souci majeur, l'épineux problème dépend de l'accessibilité de ces derniers aux contenus inadaptés.

L'absence de vérification de l'âge sur internet cause deux grandes difficultés auprès du public concerné, lequel ne s'en rend pas compte[551]. D'une part, l'enfant qui se rend sur un espace aussi vaste et libre qu'internet peut, facilement, être confronté à des contenus inadéquats et ainsi lui causer des traumatismes[552]. D'autre part, l'enfant peut, de manière crédule, compromettre son intégrité, physique ou morale, en divulguant, sans s'en rendre compte, des informations intimes (données personnelles) à son sujet[553].

Ce sont ces deux phénomènes qui sont, par exemple, dénoncés par l'association de consommateur UFC-Que Choisir, laquelle rejoint une plainte du Bureau Européen des Unions de Consommateurs à l'encontre de l'application dénommé « TikTok »[554].

L'UFC-Que Choisir alerte les internautes sur les dérives de l'application de partage de vidéo « TikTok », puisque celle-ci bafoue les droits des utilisateurs (en se réservant notamment le droit d'utiliser, modifier ou reproduire les vidéos publiées), ne protège pas ses utilisateurs les plus jeunes, ou encore, surexploite les données des utilisateurs[555].

---

551 J. Rochfeld, *Les données à caractère personnels – Les données des mineurs,* Rép. IP/IT et communication, éd., Dalloz, 2019.

552 Cf. #CaNousRegardeTous – « *La nouvelle campagne du CSA a pour objectif de réaffirmer la raison d'être de la signalétique de la jeunesse et d'inciter au dialogue. 43% des 11-13 déclarent avoir déjà accédé à des contenus choquants (…) Pourtant, plus grave encore que le fait de voir des images choquantes, c'est la trace laissée dans l'esprit des enfants qui peut avoir des conséquences. Les aider à mettre des mots sur ce qu'ils ressentent est donc primordial. C'est ce message fort qu'ont voulu exprimer le CSA et l'agence gyro :paris dans le cadre de la nouvelle campagne avec comme message ''Ce qu'ils regardent, ça nous regarde tous''* ». URL : https://fr.adforum.com/agency/9673/creative-work/34588678/ce-quils-regardent-ca-nous-regarde-tous/csa

553 « *Chaque jour, des milliers d'enfants ont accès pour la première fois à internet, ce qui les expose à une kyrielle de dangers (…). Il suffit d'un simple clic sur un lien pour qu'un enfant, quelque part, créé une trace numérique que ceux qui ne prennent pas nécessairement en compte l'intérêt supérieur de l'enfant peuvent suivre et potentiellement exploiter* », L. Chandy (Directeur des données, de la recherche et des politiques de l'UNICEF), *Plus de 175 000 enfants s'exposent à de nombreux risques sur internet chaque jour*, publié le 05 février 2018.

554 URL : https://www.beuc.eu/publications/beuc-files-complaint-against-tiktok-multiple-eu-consumer-law-breaches/html

555 URL : https://www.quechoisir.org/action-ufc-que-choisir-tiktok-depot-d-une-plainte-europeenne-contre-l-application-n88258/

C'est donc pour éviter que de telles situations ne se reproduisent que le Sénat a adopté la loi du 30 juillet 2020, laquelle renforce les pouvoirs de contrainte à l'égard des sites internet et applications qui ne mettraient pas en œuvre des conditions d'accès et ne pratiqueraient de vérifications d'âge des utilisateurs, sur leurs propres plateformes.

Certains praticiens ont pu apprécier le fait que la loi garantissait un véritable pouvoir d'injonction et de sanction cas de violation de l'article 227-24 du Code pénal[556].

192. Si la situation, en faveur des personnes qui consentent à l'utilisation de leurs données personnelles, tend à évoluer, il reste que les différentes pratiques dénoncées, précédemment, peuvent être amoindries, mais sont difficiles à anéantir. Le problème de la vérification de l'âge du consentement sur internet est un problème qui a vocation à perdurer. Pour preuve, aucune solution ne semble complètement satisfaire, pire encore, au Royaume-Uni, faute de consensus, ce combat a été, simplement, abandonné[557].

Pour autant, il faut se réjouir de cette prise de conscience. Si de nos jours, il suffit, de manière infantile, pour l'utilisateur de cliquer sur une bannière, ou de faire dérouler un menu avec des dates de naissance, pour attester qu'il est majeur, des idées germent pour le futur afin de pallier à ces problèmes.

Un temps évoqué pour remplacer les formulaires déclaratifs de majorité, qui ne nécessite qu'une simple déclaration sur l'honneur invérifiable, l'idée de l'application FranceConnect n'a pas été retenu, pas plus que l'utilisation de cartes bancaires[558].

---

556 « *La loi octroie d'ailleurs au président du CSA certains pouvoirs d'injonction et, en cas d'inexécution de l'injonction, de saisine du président du tribunal judiciaire de Paris aux fins de cessation de l'accès au service, lorsqu'il constate qu'une personne, dont l'activité est d'éditer un service de communication au public en ligne, permet à des mineurs d'avoir accès à un contenu pornographique en violation de l'art. 227-24 c. pén. (art. 23 de la loi)* », L. Mary, *Présentation de la loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales*, AJ Famille 2020, p. 384.

557 URL : https://www.lefigaro.fr/secteur/high-tech/le-royaume-uni-ne-controlera-finalement-pas-l-identite-des-usagers-de-sites-pornographiques-20191017

558 URL : https://twitter.com/benjaminhue/status/1272547570129285122 ; URL : https://twitter.com/JeanMichelMIS/status/1272552939396239360

Si le recours à la plateforme d'identification gouvernementale aurait pu être une solution technique intéressante permettant de réguler et ainsi limiter l'accès aux mineurs à la pornographie en ligne, la vérification de l'âge numérique par ce procédé aurait été, toutefois, contraignant notamment et surtout en ce que l'État aurait eu connaissance, chaque fois qu'un utilisateur se serait connecté sur un site, de l'information relative à l'orientation sexuelle de la personne concernée, ce qui est, bien entendu, contraire à l'article 9 du Règlement général de protection des données[559]. Bien qu'étant un sujet social critique, le problème de l'accès aux mineurs à des contenus inappropriés sur internet se voit pour autant relégué au second plan lorsqu'il entre en conflit avec celui relatif à la protection des données personnelles.

Une autre mesure également abordée, relative cette fois à l'utilisation de cartes bancaires, démontre aussi le conflit existant entre l'intérêt porté aux mineurs du fait des atteintes qu'ils subissent et la préservation de l'atteinte faite aux données personnelles. Si plusieurs possibilités ont été envisagées pour contrôler l'âge des utilisateurs tel que l'utilisation obligatoire de cartes bancaires pour se rendre sur un site, l'achat avec sa pièce d'identité de pass spécifiques à utiliser uniquement pour les sites spécialisés ou encore la mise en place de micropaiement symbolique, ensuite remboursé, donnant droit à l'accès à ces mêmes sites, ces mécanismes ont fait l'objet de critiques. D'un point de vue pratique, ces solutions n'étaient pas satisfaisantes puisqu'il n'était pas concevable d'interdire l'accès aux mineurs à des sites internet par l'utilisation de cartes bancaires alors que celles-ci sont disponibles et ce dès l'âge de 16 ans. D'un point de vue fiabilité, outre le fait que les personnes sont frileuses avec l'utilisation des cartes bancaires puisque cela peut, à très court terme, impacter leurs finances en cas d'atteintes, à long terme de telles dérives touchent aux finances, mais aussi et surtout aux données personnelles de ces derniers, voilà pourquoi, comme le mentionne la proposition de loi de la députée Bérangère Couillard, outre-manche, les britanniques ont abandonné l'idée d'un contrôle de l'âge des internautes pour l'accès aux contenus pornographiques au moyen de cartes bancaires, ce procédé n'étant pas conforme

[559] « *Le traitement des données à caractère personnel (…) ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits* », RGPD art. 9, *préc.*

au Règlement européen, les données des internautes pouvant être détournées de leur visée initiale[560].

En réalité, c'est, en premier lieu, par une responsabilisation des sites internet ayant obligation de proposer et de vérifier, eux-mêmes que les utilisateurs ont bien la majorité que le combat doit être mené[561]. Celui-ci doit être conjugué par un dialogue et un travail auprès des enfants, sur l'importance de leurs propres données personnelles, et cela à travers les associations, l'école ou directement au sein du foyer familial[562].

L'intelligence artificielle[563], au moyen de détection faciale pourrait être un moyen de lutter contre la problématique, mais est-ce un procédé réellement fiable ?[564] Cette solution ne crée-t-elle pas un autre problème, celui concernant le droit à l'image et la vie privée ? Que font les plateformes qui reçoivent ces « selfies » dans le but de les analyser pour vérifier l'âge des internautes ? Encore une fois, une traçabilité existe-t-elle pour ces informations transmises ?
Si le Code civil et le règlement européen sur la protection des données permettent d'identifier qu'un mineur de 15 ans est capable de consentir à l'utilisation de ses

---

560 Proposition de loi (n°2478) visant à protéger les victimes de violences conjugales, Document faisant état de l'avancement des travaux de la rapporteure, B. Couillard, 13 janvier 2020.

561 « *Jean-Jacques Bourdin : Le fournisseur, le site, va devoir mettre en place un contrôle lui-même ?*
Marie Mercier : Absolument.
Jean-Jacques Bourdin : Et s'il ne met pas en place ce contrôle, cette interdiction d'accès au mineur, il sera condamné ?
Marie Mercier : Bien sûr, jusqu'à la fermeture car la fermeture va entrainer une baisse de leur rentrer d'argent sur leur site payant », L'interview « Savoir comprendre » : M. Mercier, RMC, Bourdin Direct (6h-9h), Diffusée le 11 juin 2020.

562 « *Puisqu'elles contribuent au fondement de leurs identités numériques au sens large, le Conseil recommande d'informer les citoyens sur leurs droits vis-à-vis de leurs données personnelles. En plus d'un apprentissage sur le long terme à destination de élèves du primaire et du secondaire, le Conseil recommande qu'un budget soit alloué à la CNIL pour réaliser des campagnes de communication sur les données personnelles dans des grands médias et à des heures de grande écoute* », Rapport du Conseil national du numérique, Identités numériques : Clés de voute de la citoyenneté numérique, Juin 2020, p.14.

563 S. Chatry et A. Robin, *Introduction à la propriété intellectuelle, Op cit*, n° 123.

564 « *On a tendance à l'oublier mais Snapchat, TikTok, Instagram, Whatsapp, Facebook, toutes ces applications sont interdites au moins de 13 ans et pourtant les 10-12 ans sont de plus en plus nombreux à s'y inscrire, parce que, tout simplement, c'est très simple, il suffit de mentir sur sa date de naissance. D'où cette idée d'utiliser l'intelligence artificielle pour analyser leurs visages à l'inscription et en déduire leurs âges* ». A. Mbida, *L'intelligence artificielle pour vérifier l'âge sur Internet*, L'innovation du jour, Chronique de l'émission Europe Matin – 5h-7h, Diffusée le Jeudi 14 novembre 2019.

données personnelles, il ne faut, toutefois pas oublier qu'internet représente une sphère dangereuse[565]. A court terme, des milliers de contenus non adaptés peuvent choquer et traumatiser les enfants. A long terme, des personnes peu scrupuleuses peuvent profiter de la fragilité de certains individus pour récupérer des informations intimes et privées sur eux et ce pour diverses raisons, souvent très malintentionnées.

193. Aussi, après avoir répondu à la question de savoir qui peut consentir à l'utilisation de ses « données personnelles », il convient de se demander quelles sont les modalités du consentement dans le but de répondre à la question de savoir comment consentir ?

Au sein de son considérant 32, le règlement général impose que le consentement soit donné par un acte « *positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant* »[566]. En tant qu'acte « positif », il devra donc être un acte volontaire de la part de l'utilisateur. Il sera, alors, formellement prohibé et donc sanctionné, pour tout responsable de traitement de recueillir le consentement d'une personne par des pratiques dites d'*opt-in* passif qui consiste à obtenir le consentement d'un internaute de manière détournée, par exemple en utilisant des cases déjà « pré-cochées »[567].

De plus, puisque le consentement doit être recueilli de façon « libre, spécifique, éclairée et univoque », cela interdit tout recours ou méthode visant à « noyer » d'informations l'utilisateur et ainsi obtenir le consentement de ce dernier sans qu'il s'en aperçoive[568].
De ce fait, les techniques paradoxales, telles que celles de « consent fatigue »[569], pourtant abondements pratiqués par, les sites internet, notamment, dans le but

---

[565] J. Rochfeld, *Les données à caractère personnels – Les données des mineurs, Op cit*.
[566] RGPD consid. 32, *préc*.
[567] *V. supra §n°121.*
[568] *V. supra §n°118.*
[569] « *Afin de protéger les internautes, la règlementation européenne relative à la protection des données impose, en principe, le consentement pour l'utilisation de traceurs sur l'appareil de l'utilisateur. C'est pour cela qu'aujourd'hui, lorsqu'un internaute arrive sur un site web ou une application mobile, une*

d'obtenir un consentement pouvant être qualifié de consentement « obtenu à l'usure », ne remplissent pas les conditions posées par le règlement. Pour autant, comment reprocher à certains utilisateurs d'accepter, par défaut et donc de consentir à l'utilisation de leurs propres données, parce que découragées par certaines pratiques ?[570]

Ce phénomène est courant et certains auteurs constatent qu'il existe aujourd'hui « *une forme de lassitude chez des utilisateurs qui cliquent de plus en plus mécaniquement sur le fameux ''Tout accepter''* »[571].

194. En ce qui concerne la forme même du consentement, ce dernier pourra valablement être requis « *au moyen d'une déclaration écrite, par voie électronique ou d'une déclaration orale* »[572]. Le plus simple pour le responsable de traitement serait donc d'insérer une case « oui » et une case « non », l'action de cocher l'une ou l'autre des cases validant ou rejetant le consentement de la personne concernée.

Il convient enfin d'énoncer que si le consentement est un acte « positif », *a contrario*, ce ne peut pas être un acte « négatif ». Le consentement par silence, par défaut ou inactivité ne serait, donc, être valablement accueilli puisqu'il serait contraire au présent règlement.

195. Outre les problématiques de capacité et les questions relatives aux modalités du consentement, lorsque celui-ci est en lien avec l'utilisation de données personnelles, il est nécessaire de rappeler que si celui-ci est un élément fondamental du règlement européen et des données personnelles en général, en ce

---

bannière apparait pour permettre le paramétrage des traceurs. Or, la multiplication de ces bannières, si elle a permis de rendre plus visible l'existe des traceurs, aboutirait, selon certains à une « fatigue du consentement » qui signifierait, selon eux, que les internautes ne souhaitent pas que leur accord leur soit demandé », URL : https://www.cnil.fr/fr/publicite-ciblee-en-ligne-quels-enjeux-pour-la-protection-des-donnees-personnelles

570 *« Le consent fatigue est une pratique ou les consommateurs jouent à un jeu d'enfant avec des notifications de consentement sans prendre le temps de les comprendre. Plutôt que de donner du pouvoir aux consommateurs, le modèle actuel les aveugle sur ce que signifie la confidentialité des données. Il est plus simple de cliquer simplement sur ''Accepter'' et de continuer »,* URL : https://marketoonist.com/2019/05/data-privacy-consent-fatigue-and-gdpr.html

571 URL : https://comarketing-news.fr/rgpd-user-loser/

572 RGPD consid. 32, *préc.*

qu'il « *assure aux personnes concernées un contrôle fort sur leurs données* »[573], il n'est pas, pour autant, une étape automatique et inéluctable.

Un retour sur l'intérêt et le crédit apporté au consentement propice à l'utilisation de données personnelles permet de s'en convaincre.

Pour mémoire, l'article 6 (1) du présent règlement détermine le champ d'application de la licéité du traitement des données personnelles à travers six bases légales[574]. Bien que très important et non négligeable, c'est une erreur de penser que « *le recueil du consentement de la personne concernée est la condition sine qua non du traitement de ses données* »[575]. En effet, faisant partie des six fondements ou bases juridiques possibles, « *le consentement n'est donc qu'un fondement au traitement parmi d'autres* »[576]. Plus encore, pour certains, « *Tout au plus, le consentement n'est que l'une des six bases légales sur lesquels un traitement doit nécessairement se fonder* »[577]. L'utilisation du terme « *Tout au plus* » démontre que le consentement, en plus d'être descendu de son piédestal, est placé au même rang que les autres bases légales, voir même, est relégué au second plan[578].

Une approche, radicale, est enfin suggérée à propos de la requête du consentement et de sa portée, à savoir que certains spécialistes préconisent, étonnament, de ne pas demander le consentement des personnes concernées[579]. Pour comprendre

---

[573] URL : https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes

[574] *V. supra §n°73 et 74.*

[575] URL : ttps://www.digitemis.com/blog/rgpd-quelle-base-juridique-pour-vos-traitements-de-donnees-a-caractere-personnel/

[576] « *Une idée largement répandue voudrait que le nouveau cadre de protection des données personnelles posé par le RGPD implique un recueil, sinon systématique, du moins très fréquent, du consentement des personnes concernées avant de pouvoir mettre en œuvre un traitement* », D. Conerardy et A. Ramel, *RGPD et consentement, un malentendu handicapant pour les acteurs publics*, Le courrier des maires – n° 335-336, Juin-Juillet 2019, p. 36.

[577] C-E. Armingaud, *Le consentement : le faux-ami des bases légales ?*, (2019), Revue Lamy droit de l'immatériel (n° 160, 2019), p. 44.

[578] « *Le consentement est l'une des six bases juridiques qui fondent le traitement. S'il est le premier fondement énoncé par l'article 6 du RGPD, il n'est pas nécessairement celui qui doit être préféré par les responsables de traitement* », F. Rogue, *Capacité et consentement au traitement de données à caractère personnel et au contrat, Op cit*, p. 370.

[579] « *Arrêtez de demander le consentement (…), ce n'est jamais que l'une des six bases légales que vous devez utiliser. Dans certains cas vous devez traiter les données à caractère personnel et donc il est hors de question de demander le consentement aux personnes dont les données sont traitées* », URL : https://www.donneespersonnelles.fr/consentement-rgpd-valable

cette suggestion, il faut imaginer que ce qu'il adviendrait si l'administration fiscale était tenue de demander le consentement des personnes. La conclusion, logique, serait que peu de monde ne paierait l'impôt.

Le traitement de données étant, le plus souvent, fondée par une obligation légale qui s'impose de par sa nature, ainsi il n'est pas, systématiquement, essentiel de recueillir le consentement des personnes concernées. Concrètement, en entreprise par exemple, il n'est pas nécessaire ni obligatoire de recueillir le consentement de ses salariés[580], pour le traitement de leurs données personnelles, des lors qu'une obligation légale oblige à une telle action.

La pratique consistant à ne pas demander le consentement des personnes concernées, lorsque cela est autorisé, légalement prévu, permet d'éviter certaines situations problématiques et confuses[581]. C'est par exemple le cas en entreprise dans le cas de figure suivant à savoir que, après avoir demandé le consentement de nombreux salariés d'une entreprise, si ces derniers usent de leur droit de retrait, cela peut paralyser totalement le bon fonctionnement de celle-ci[582]. S'il ne faut pas omettre le fait que le consentement n'est pas obligatoire[583], ce dernier ne doit, toutefois, pas être négligé.

196. L'utilisation du consentement, comme élément fondateur au traitement des données personnelles, est non-impérieuse, mais la portée de ce mécanisme reste bien réelle. La sécurité des données personnelles, cheval de bataille du règlement

---

580 *V. supra §n°131 et 132.*

581 « *Il peut, en effet, y avoir des ''effets pervers'' dans la prévalence que pourrait prendre le consentement, car si le consentement ne répond pas aux caractères énoncés par le règlement, ou si ce consentement est retiré, le traitement sera ipso facto illicite* », F. Rogue, *Capacité et consentement au traitement de données à caractère personnel et au contrat*, *Op cit*, p. 370.

582 « *De plus, comme Rowenna Fielding l'écrit dans son blog, si une personne concernée retire son consentement et que vous réalisez ensuite que vous avez une obligation légale de continuer le traitement des données, vous vous retrouvez dans une situation sans issue* », S. Meunier, *RGPD : Quand devez-vous obtenir le consentement*, 1er Septembre 2017.

583 « *So, let me start by saying GDPR does not make consent a mandatory requirement for all processing of personal data* »,
« *Permettez-moi donc de commencer par dire que le RGPD ne fait pas du consentement une exigence obligatoire pour tout traitement des données personnelles* », R. Fielding, *What the GDPR does – and doesn't – say about consent*, Miss IG Geek Blog, Privacy and information geek for hire, 31 Mai 2017.

pour la protection des données, est notamment renforcée lorsque la condition du consentement est utilisée. En effet, l'un des buts, majeurs, de ce règlement est d'aider, protéger, les personnes concernées par l'utilisation de leurs données personnelles, contre les organes de traitement, les GAFA, les puissants de l'informatiques qui usent de leur position de force. La place du consentement en matière de protection des données se doit d'être, « *la condition cardinale du régime de traitement des données* »[584]. Aussi, pourquoi se priver d'utiliser une-t-elle mesure, même si celle-ci n'est pas obligatoire ?

[584] C. Castets-Renard, *Brève analyse du règlement général de la protection des données*, Dalloz IP/IT 2016, p. 311.

CONCLUSION DU CHAPITRE 2

Lorsque le consentement est recueilli en faveur d'un contrat portant sur l'utilisation de la donnée personnelle, en théorie un lien existe entre le consentement au contrat et le consentement à l'utilisation de la donnée personnelle, bien qu'en pratique quelques distinctions subsistent.

C'est la raison pour laquelle, le consentement à l'utilisation de la donnée personnelle bénéficie de certaines modalités qui lui sont propres.

CONCLUSION DU TITRE 2

197. Le consentement est un des ciments du contrat lorsque celui-ci est en lien avec les données personnelles.

Que le contrat porte directement sur une donnée personnelle ou bien qu'il porte sur l'utilisation de celle-ci, le consentement donné ne sera pas le même.

198. Confronté directement à la notion de donnée personnelle, le consentement repose sur l'obligation spécifique d'information propre à chaque contrat comme il en est, par exemple, du contrat médical ou du contrat de travail.

Lorsqu'il porte sur l'utilisation de la donnée personnelle, le consentement n'est plus semblable à celui donné pour un contrat de droit commun. La distinction relève, en effet, du fait que le consentement doit porter sur l'utilisation de la donnée et non plus sur la donnée personnelle elle-même.

CONCLUSION DE LA PREMIERE PARTIE

199. Il ressort de cette première partie que la donnée personnelle n'est pas, lors de la formation du contrat, un élément anodin. En effet, celle-ci, qu'elle soit l'objet du contrat ou qu'elle soit un élément de son contenu, n'est pas une « chose » à proprement parler.

200. Si sa nature juridique laisse parfois planer des doutes, les précisions apportées par l'article 4 du règlement général sur la protection des données ne résolvent pas pour autant toutes les difficultés que peut présenter un contrat qui porte, à titre principal ou accessoire, sur des données personnelles.

201. Encore très marqué par le classicisme du XIX^{e} siècle, dont il tente pourtant de s'affranchir, le droit français des contrats demeure assez perplexe face à des « choses » dématérialisées au premier rang desquels se place « l'information » visée par le règlement européen d'avril 2016.

Cela crée des incertitudes dans l'analyse du contrat sur les bases de sa formation, cela génère, de ce fait, des difficultés dans son exécution.

DEUXIEME PARTIE

L'exécution du contrat portant sur les données personnelles

202. Pour ce faire, il convient d'étudier la vie du contrat portant sur les données personnelles dans son ensemble, ce qui implique, tour à tour, de s'intéresser à l'exécution des contrats portant sur les données personnelles (Titre I), puis à l'inexécution des obligations portant sur les données personnelles (Titre II).

TITRE 1

L'exécution des contrats portant sur les données personnelles

203. L'étude de l'exécution des contrats portant sur les données personnelles est celle des obligations en lien avec l'utilisation des données personnelles (Chapitre 1), mais aussi et surtout celle des obligations dont la finalité est en lien avec la protection de la donnée personnelle (Chapitre 2).

Chapitre 1 : Les obligations en lien avec l'utilisation des données personnelles

204. L'analyse des obligations en lien avec l'utilisation des données personnelles se fait au travers de la finalité des contrats portant sur l'utilisation de la donnée personnelle (Section 1) et au travers des différentes modalités propres à l'utilisation de la donnée personnelle (Section 2).

Section 1 : La finalité des contrats portant sur l'utilisation de la donnée personnelle

205. Afin de comprendre ce qu'est réellement la finalité des contrats portant sur l'utilisation de la donnée personnelle, il convient de s'attacher à la détermination positive (Paragraphe 1) et négative (Paragraphe 2) de ces derniers.

§1 La détermination positive des obligations liées à l'utilisation de la donnée personnelle

206. Une fois encore, il convient de s'intéresser aux hypothèses choisies précédemment, celles du contrat de santé ou du contrat de travail.

207. En matière de santé, il existe une illustration assez claire du champ de l'autorisation de l'utilisation de la donnée de santé. Bien que relevant du domaine de l'intimité des personnes, l'utilisation de la donnée personnelle est autorisée par le Règlement général sur la protection des données si elle relève d'une activité de recherche[585] : ainsi, si l'utilisation de la donnée est rendue nécessaire à des fins de médecine préventive, de diagnostics médicaux, de l'administration de soins ou de traitements, ou encore de la gestion de services de santé et mise en œuvre par un membre d'une profession de santé, ou par une autre personne soumise à l'obligation de secret professionnel, alors elle sera possible[586].

De la même manière, et toujours à des fins scientifiques, elle sera rendue possible si elle est conforme à la loi Informatique et libertés et justifiée par l'intérêt public, pour éviter notamment la propagation des maladies, ou dans le cadre d'une recherche publique, après avis motivé et publié de la Commission nationale de l'informatique et des libertés, ou encore s'il s'agit de données rendues anonymes.

---

[585] « *Pour faciliter la recherche scientifique, les données à caractère personnel peuvent être traitées à des fins de recherche scientifique sous réserve de conditions et de garanties appropriées prévues dans le droit de l'Union ou le droit des États membres* », RGPD consid. 157, *préc.*

[586] *V. déjà en ce sens art. L. 1110-4 al. dernier du CSP*, *préc.*

208. Bien plus que d'être seulement autorisée ou rendue possible, les activités de recherche scientifique et médicale, au même titre que celles réalisées à des fins archivistiques, sont encouragées par le règlement européen au moyen d'un régime dérogatoire.

En premier lieu, par l'instauration d'un tel régime, le présent règlement a pour objectif de faciliter les traitements de données personnelles en matière médicale et scientifique dont la finalité à vocation à profiter à l'intérêt général.
Une seconde raison explique et justifie la création d'un régime aux conditions bien moins contraignantes, à savoir qu'un tel mécanisme profite indirectement à la recherche médicale et scientifique puisqu'il permet d'éviter toutes situations de dépendances, à des tiers ou à des plateformes privées, pour l'accès aux données personnelles. Le cas de « Facebook » démontre la crainte précédente, à savoir que cette firme, dans le but de se repentir suite au scandale de l'affaire « Cambridge Analytica »[587], a décidé de libérer certaines données personnelles afin d'étudier l'influence des réseaux sociaux sur la démocratie[588]. Si dans cet exemple, les données personnelles étaient seulement transmises, gratuitement, à des fins scientifiques, il faut imaginer que ce genre de pratique peut entrainer certaines dérives, notamment la monétisation et la marchandisation des données. Aussi, faciliter l'utilisation de données personnelles dans le domaine scientifique ou médical, c'est accorder plus d'indépendance aux responsables de traitement qui s'en occupent et c'est permettre d'éviter que la récolte des données devienne monétisée, ce qui est contraire aux principes de médecine et de science.
S'intéresser au régime dérogatoire de l'utilisation des données personnelles en matière de santé revient à s'intéresser aux allègements des obligations concernant les formalités dites préalables. Si le règlement général sur la protection des données admet certains assouplissements, dans l'intérêt de développer et d'améliorer le domaine de la santé, il existe tout de même un contre-pied. En effet, afin de compenser un régime de traitement et d'utilisation des données personnelles, en matière de santé, peu strict et peu contraignant, la logique de

[587] *V. supra §n°93.*

[588] URL : https://www.lebigdata.fr/facebook-donnees-reseau-democratie

responsabilité des responsables de traitement est quant à elle renforcée[589]. Si d'une part, il est possible de se réjouir de la réduction des contraintes à propos d'utilisation des données personnelles en matière de santé, d'autre part, il est sécurisant, pour les individus et leurs données personnelles, d'avoir transféré le principe de responsabilité sur les acteurs de traitement des données. Cette substitution du contrôle des risques représente un équilibre, non négligeable, entre l'indépendance pour l'activité de recherche médicale et l'impératif de protection des droits fondamentaux des personnes concernées.

Si le règlement européen consent quelques libertés et permet des règles plus adoucies dans l'optique d'encourager et de soutenir les activités de recherche médicale par l'utilisation des données personnelles, il n'en oublie pas son objectif principal de protection des personnes concernées. Aussi, le régime dérogatoire est favorablement accueilli en ce qu'il ne porte pas atteinte ni aux droits fondamentaux, ni aux données personnelles des individus[590]. Pour légitimer son action, le règlement UE 2016/679 souligne de manière explicite l'importance et l'intérêt pour la société des traitements reposant sur l'utilisation de données personnelles à des fins de recherche scientifique ou médicale[591] et insiste sur la légitimité des activités de recherche, sous réserve qu'elles respectent les conditions de protection des données personnelles fixées par le règlement[592].

Il faut dépasser l'alinéa 1[er] du considérant 159[593] du règlement général sur la protection des données pour avoir enfin une définition concrète de ce qu'est la recherche scientifique et pour en déterminer un périmètre. En effet, ce terme

---

589 « *En contrepartie de la suppression de certaines formalités, le responsable de traitement doit être en mesure de démontrer, à tout moment, sa conformité aux exigences du RGPD en traçant toutes les démarches entreprises (principe d'accountability)* », URL : https://www.cnil.fr/fr/quelles-formalites-pour-les-traitements-de-donnees-de-sante-caractere-personnel

590 « *Le traitement des données à caractère personnel à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques devrait être soumis à des garanties appropriées pour les droits et libertés de la personne concernée, en vertu du présent règlement* », RGPD consid. 156, *préc.*

591 RGPD consid. 157, *préc.*

592 « *Lorsque des données à caractère personnel sont traitées à des fins de recherche scientifique, le présent règlement devrait également s'appliquer à ce traitement* », RGPD consid. 159, *préc.*

593 *Ibid.*

recouvre bon nombre d'activités telles que « *le développement et la démonstration de technologies, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé (...). Il convient également d'entendre les études menées dans l'intérêt public dans le domaine de la santé publique* » et doit donc être entendu dans un sens large et ce sans distinction de caractère, c'est-à-dire une recherche scientifique et médicale aussi bien privée que publique.

209. Il convient désormais de présenter une des nombreuses facultés prévues par le régime dérogatoire, lui-même institué par le règlement européen, afin de démontrer l'intérêt que ce dernier porte à l'utilisation des données personnelles confrontées au secteur médical.

Il est question de souplesse quant à l'admission de certaines indéterminations des finalités des traitements à des fins de recherche. En effet, si l'article 5 (1.b) du présent règlement affirme que les données personnelles ne sont collectées que pour certaines finalités bien précises[594], définies en amont, puis, par la suite, portées à la connaissance des personnes concernées (article 13 et 14 du Règlement général sur la protection des données)[595], le considérant 33[596], de ce même règlement, déroge à la règle en prévoyant et en admettant qu'en matière scientifique et médicale, l'exception existe puisqu'il n'est pas toujours possible de déterminer à l'avance la finalité exacte d'un tel traitement.

Cette dérogation offre aux responsables de traitements, c'est-à-dire les chercheurs du domaine scientifique et médical, une marge de manœuvre pour l'élaboration des finalités d'utilisation et de traitements des données personnelles. Cette

---

[594] « *1. Les données à caractère personnel doivent être : b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités* », RGPD art. 5 (1.b), *préc.*

[595] RGPD art. 13 et 14, *préc.*

[596] « *Souvent, il n'est pas possible de cerner entièrement la finalité du traitement des données à caractère personnel à des fins de recherche scientifique au moment de la collecte des données. Par conséquent, les personnes concernées devraient pouvoir donner leur consentement en ce qui concerne certains domaines de la recherche scientifique, dans le respect des normes éthiques reconnues en matière de recherche scientifique. Les personnes concernées devraient pouvoir donner leur consentement uniquement pour ce qui est de certains domaines de la recherche ou de certaines parties de projets de recherche, dans la mesure où la finalité visée le permet* », RGPD consid. 33, *préc.*

largesse vient, notamment, du fait que le domaine de la recherche est imprévisible et en constante évolution, il est donc compréhensible que certaines commodités lui soient accordées. L'exception présentée, qui représente l'unique exemple par lequel le règlement général sur la protection des données conçoit une indétermination de la finalité initiale d'un traitement de données, ce qui est normalement un principe fort gage de sécurité pour les personnes concernées, est la preuve que le règlement européen agit avec bienveillance à l'égard du domaine de la santé.

La recherche scientifique et médicale est un domaine au sein duquel l'utilisation de données personnelles est fortement employée. Cette pratique, en plus d'être autorisée est également encouragée. L'utilisation de données personnelles s'accorde parfaitement avec l'activité de recherche en ce qu'elle permet de nombreuses avancées, ayant vocation à profiter à tous, voilà pourquoi le traitement de ces données dispose de quelques facilités. La détermination positive des obligations liées à l'utilisation de la donnée personnelle étant réalisée au prisme du contrat de santé, il convient, à présent, de s'intéresser à un domaine voisin, le contrat de travail.

210. S'agissant d'une relation de travail, là encore, le règlement général sur la protection des données encadre ce domaine et prévoit à quelle fin il est possible d'utiliser les « données personnelles » des salariés. En effet, cette exigence essentielle se retrouve à l'article 6 dudit règlement et conditionne la licéité du traitement si ce dernier est nécessaire à l'exécution d'un contrat[597].

Cette précision étant apportée, il convient d'en tirer la conséquence suivante, à savoir que pour les traitements de données personnelles effectuées au sein de l'entreprise, il ne sera pas nécessaire de recueillir le consentement des salariés[598],

[597] RGPD art. 6, *préc.*

[598] « *L'employeur ne doit pas recueillir le consentement exprès de ses salariés pour mettre en œuvre la plupart des traitements de données personnelles dans son entreprise* », URL : https://www.village-justice.com/articles/les-nouvelles-obligations-employeur-matiere-protection-des-donnees-personnelles,28756.html

le contrat de travail moteur de la relation employeur/employé suffisant, à lui seul, pour justifier une telle activité.

211. En matière de droit du travail, deux cas de figure permettent de mettre en lumière la détermination positive des obligations liées à l'utilisation de la donnée personnelle. En effet, concernant un contrat de travail, le traitement de données personnelles est nécessaire d'une part dans le cadre d'une relation précontractuelle, ce qui correspond à la période de recrutement[599], mais il est également indispensable, d'autre part, dans le cadre de l'exécution du contrat avec la personne concernée, en l'occurrence un salarié, ce qui correspond à la gestion du personnel.

Premièrement, dans le cadre d'un recrutement, il sera possible, pour un potentiel employeur, de prélever toutes les « données personnelles » permettant d'évaluer la capacité du candidat à occuper l'emploi proposé. C'est le cas pour toutes les informations en lien avec la qualification du candidat (niveau d'étude, diplômes ou encore le type de permis, si cela est en lien avec le poste à pourvoir).

Au moment de l'embauche du candidat, il sera également possible pour l'employeur confirmé de collecter des informations complémentaires utiles, pour l'avenir, à la gestion du personnel. Outre les informations nécessaires au respect d'obligation légale, tel que le numéro de sécurité sociale, permettant d'effectuer les déclarations sociales obligatoires[600], l'employeur pourra enfin demander des informations utiles à la gestion administrative du personnel (par exemple les coordonnées de personnes à prévenir en cas d'urgence), à l'organisation du travail (par exemple une photographie de l'employé pour réaliser les organigrammes de l'entreprise), ou encore à l'action sociale prise en charge par l'employeur (par exemple, les informations concernant les ayants-droits de l'employé).

---

[599] « *Processus incontournable de la vie de l'entreprise, le recrutement correspond à l'ensemble des actions mises en œuvre pour trouver le candidat qui correspond aux exigences de compétences (savoirs, savoir-faire et savoir-être) et de qualifications (diplômes et titres) requises pour un poste donné* », URL : https://www.droit-travail-france.fr/processus-recrutement.php

[600] RGPD art. 9 (2. b), *préc.*

Ensuite, lorsque la relation de travail entre un employeur et un employé est établie, il sera possible pour le premier de collecter et d'utiliser les « données personnelles » relatives à son salarié si, et seulement si, leurs utilités sont nécessaires pour le bon déroulement du contrat en question (contrat de travail entre l'entreprise et le salarié).

212. Pour imager les propos précédents, il est possible de s'intéresser à une nouvelle forme de travail démontrant, une nouvelle fois, la détermination positive des obligations liées à l'utilisation de la donnée personnelle.

En effet, depuis la crise et les confinements successifs, le télétravail s'est développé et s'est imposé comme nouvelle organisation de travail. A ce titre, si les employés utilisent des outils informatiques appartenant aux entreprises, des fragments de leurs données personnelles ne sont pas pour autant épargnés. Aussi, s'il est possible pour un employeur, en qualité de responsable de traitement, de disposer, librement, des données personnelles de ses salariés, celui-ci devra justifier des moyens mis en œuvre, pour ce faire, afin de veiller au respect de la vie privée des salariés[601], une telle logique est, également, prévue par le règlement européen à travers l'obligation de loyauté[602]. Ainsi, les entrepreneurs ne peuvent contrôler l'activité de leurs salariés, à travers l'outil informatique, que lorsque cela est pleinement nécessaire. Attention, pour ce faire, l'employeur devra informer le salarié[603] (de l'identité du responsable de traitement, des données qui seront collectées, de la durée de conservation ou encore des destinataires) pour motiver les raisons d'un tel contrôle.

La surveillance des salariés à distance n'est donc pas incompatible avec la détermination positive propre à l'utilisation des données personnelles, pour autant celle-ci est encadrée, le respect de la vie privée des salariés devant primer.

---

601 « *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* », C. trav., art. L. 1121-1, *préc.*

602 « *1. Les données à caractère personnel doivent être : a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence)* », RGPD art. 5 (1.a), *préc.*

603 RGPD art. 13, 14 et 15, *préc.*

213. La question de l'utilisation des données personnelles ne concerne pas seulement, la naissance de la relation de travail ou l'exécution de celle-ci, mais intéresse également une dernière phase relative, cette fois, à fin du contrat de travail. En effet, puisque le contrat de travail est la base légale qui justifie le traitement de données des salariés, qu'en est-il lorsque cette relation cesse ? Concernant cette problématique, si l'article 17[604] du règlement général sur la protection des données personnelles impose aux responsables de traitement un droit à l'effacement des données personnelles (ou droit à l'oubli) qui profite aux salariés, il sera tout de même possible pour l'employeur de conserver lesdites données quand elles sont nécessaires à la défense des droits en justice ou si elles sont liées à un accident de travail[605]. A titre d'exemple, une autre forme d'archivage des données personnelles est, de la même façon, légalement prévue, le Code du travail obligeant, sous certaines conditions, les employeurs de conserver les bulletins de paie[606].

Dans ces situations, l'employeur sera donc autorisé à collecter et conserver les données de ses propres salariés et ce même lorsque ces derniers ne travaillent plus au sein de l'entreprise. Cette possibilité n'est pas dérangeante, l'employeur ayant déjà les données personnelles des salariés, ou ex salariés, en sa possession lorsqu'ils faisaient partie de l'entreprise, il n'y a, de ce fait, aucun inconvénient à ce qu'il les conserve pendant un temps limité, cette conservation étant justifiée par d'éventuelles actions juridiques.

214. Le lien qui existe entre les informations personnelles des salariés et l'utilité que peut en avoir un employeur peut présenter un intérêt majeur et il peut être nécessaire de poser les règles d'un certain contrôle, mais, pour autant il ne faut pas en abuser. Voilà pourquoi l'utilisation des « données personnelles » dans le cadre d'une relation de travail est en réalité conditionnée aux critères de nécessité et de finalité.

---

604 « *La personne concernée a le droit d'obtenir du responsable de traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais* », RGPD art. 17, *préc.*

605 « *Les mentions portées sur le registre unique du personnel sont conservées pendant cinq ans à compter de la date à laquelle le salarié ou le stagiaire a quitté l'établissement* », C. trav., art. R. 1221-26.

606 « *L'employeur conserve un double des bulletins de paie des salariés pendant cinq ans* », C. trav., art. L. 3243-4.

§2 La détermination négative des obligations liées à l'utilisation de la donnée personnelle

215. En prenant le cadre spécifique dans un cadre contractuel de l'utilisation de la donnée dans le champ du droit de la santé, il existe une analyse particulièrement pertinente de ce qui peut ne peut pas être fait.

En effet, une donnée de santé est une donnée « hyper protégée » en ce qu'elle se rapporte à l'état de santé, physique ou mental, passé, présent ou futur, d'une personne physique identifiée ou identifiable[607].

Elle est collectée dans un champ conventionnel, à savoir dans le cadre du contrat d'hospitalisation ou de soins, à l'occasion d'une prestation de soins, de santé, d'une prise en charge sanitaire, ou même dans le cadre d'un contrat de recherche. Elle concerne des données aussi précieuses que le génome de la personne, sa fréquence cardiaque moyenne ou son analyse sanguine, les informations relatives à un handicap, un risque de maladie, des antécédents médicaux, un traitement clinique, un état physiologique ou biomédical, etc. Son spectre est très large, car une donnée de base (nombre de pas journaliers) peut être qualifiée de donnée de santé dès qu'on la croise avec d'autres données (âge, sexe et habitudes alimentaires) permettant de déduire l'état de santé d'une personne.

C'est pourquoi elle est particulièrement protégée, comme le rappelle le Règlement général sur la protection des données personnelles qui définit une nouvelle notion qui est la « *privacy by design* »[608]. Cela signifie qu'étant considérées comme particulièrement sensibles, les données de santé bénéficient d'un régime de protection renforcée. Le principe est simple : c'est celui d'une interdiction du traitement des données de santé relatives à une personne identifiée ou identifiable

---

607 *V. art. L. 1111-7 du CSP, préc.*

608 « *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 techniques et organisationnelles appropriées (..) destinées à mettre en œuvre les principes relatifs à la protection des données (…) de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée* », RGPD art. 25, *préc.*

à des fins de commercialisation[609], ce qu'affirmait déjà en 1997 la Commission nationale de l'informatique et des libertés[610], le règlement européen reprenant, naturellement cet avertissement, ayant, avec le développement du numérique, encore plus de force et de sens aujourd'hui. Aucune donnée collectée dans le cadre d'une activité sanitaire ne pourra donner lieu à une utilisation pécuniaire à visée commerciale.

Il est alors possible de se demander quel est le champ de cette interdiction et si cela signifie qu'aucun accord ne peut être conclu les concernant ? Il est évident que le principe de la prohibition est à nuancer. En effet, leur exploitation est, toutefois, possible si la personne concernée, bien informée de la finalité du cadre dans lequel ses données seront utilisées, donne son consentement « *clair et explicite* »[611], ce qui renvoie aux conditions déjà énoncées dans l'article L. 1111-4 du Code de la santé publique[612].

216. L'interdiction de commercialisation des données de santé est donc la première détermination négative liée à un tel traitement, elle s'explique principalement pour deux raisons, qui peuvent être assimilées. En effet, l'activité de commercialisation des données de santé reviendrait à monétiser celles-ci, ce qui aurait pour conséquence, d'une part, de sérieusement compliquer la recherche scientifique et médicale, et d'autre part, de menacer sévèrement l'intégrité des données personnelles des individus.

Pour se rendre compte du fléau que représenterait la commercialisation des données, il est possible d'imaginer les conséquences d'un tel comportement face à une crise sanitaire. Lors d'une telle hypothèse, pour limiter la propagation de virus, il est question de suivi de l'épidémie, à travers l'évolution de la santé des individus, notamment sur des critères divers est variés, âge, sexe, antécédents

---

609 RGPD art. 9 (1.), *préc* ; V. également Art. 6, Loi n°78-17 du 6 janvier 1978, *préc.*

610 « *Rappelle que les données de santé à caractère personnel ne peuvent être utilisées que dans l'intérêt direct du patient et, dans les conditions déterminées par la loi, pour les besoins de la santé publique et que, dès lors, leur exploitation à des fins commerciales doit être proscrite. En conséquence, ces données ne peuvent être traités que dans le respect des droits des personnes et des règles déontologiques en vigueur* », Délibération 97-008 du 04 février 1997.

611 RGPD art. 7, *préc.*

612 CSP., L. 1111-4, *préc*.

médicaux, afin de se préparer à toutes éventualités. Que se serait-il passé s'il avait fallu payer pour obtenir de telles informations ? La commercialisation des données est aux antipodes de ce que représente la recherche scientifique et médicale. Le fait que des plateformes privées qui détiennent des données de vendent celles-ci, au plus offrant, entrainerait à une recherche scientifique et médicale élitiste, mais pire encore cela provoquerait un blocage. L'activité de recherche représente en soi un cout faramineux qui exploserait à cause de l'obligation d'achat de données personnelles de santé pour faire avancer celle-ci, et cela pour l'intérêt général. La commercialisation des données entrainerait la création d'enchères ou seuls les plus offrants bénéficieraient des avancées scientifiques et médicales.

Concernant les individus maintenant, le fait de vendre ses propres données entrainerait un abandon total de sa vie privée. Les acheteurs de données, quel qu'ils soient, profiteraient de la situation pour déposséder les personnes de leurs données et ainsi les revendre afin d'en tirer profit. La rémunération des données de santé porterait, sans nul doute, atteinte à la vie privée des personnes. Le lien de causalité entre les difficultés causées aux personnes et celles causées à la recherche est évident, l'interdiction du commerce des données de santé étant la seule issue possible dans l'intention d'éviter toutes dérives. Si la donnée de santé est propre à chacun, son impact, notamment les biens faits qu'elle peut engendrer pour l'avancée de la recherche scientifique et médicale à, quant à elle, vocation à profiter à tous.

217. Dans la continuité de l'idée précédente, une autre restriction permet de déterminer négativement les obligations relatives à l'utilisation des données de santé, toujours dans un souci de protection de celles-ci. Il s'agit cette fois de développer l'interdiction de transfert de données de santé hors de son continent d'origine. Cette décision intervient à la suite d'observations de la commission nationale de l'informatique et des libertés à propos de la plateforme des données de santé (PDS) également appelée « Health Data Hub » ayant vocation à centraliser l'ensemble des données du système national des données de santé[613]. En qualité de responsable de traitement au sens du règlement européen, cette

[613] CSP., art. L. 1461-1.

plateforme a fait le choix de recourir à un sous-traitant, en l'espèce la société « Microsoft », pour l'hébergement informatique des données de santé en sa possession. Une requête en référé déposée par le Conseil national du logiciel libre (CNLL) sollicitait l'arrêt du traitement et la centralisation des données en lien avec l'épidémie de Covid19 sur la Plateforme des données de santé, « Health Data Hub », afin d'éviter toute atteinte grave et manifestement illégale au droit à la vie privée et à la protection des données personnelles[614]. Sur ce point, la Commission nationale de l'informatique et des libertés a appelé le gouvernement à une extrême vigilance s'agissant des conditions de conservation et des modalités d'accès aux données, et a recommandé que, à plus long terme, l'hébergement et les services de gestion de la Plateforme de santé puissent être « *réservés à des entités relevant exclusivement des juridictions de l'Union européenne* »[615]. Conscient des difficultés et des enjeux en présence, le gouvernement, par l'intermédiaire d'Olivier Véran, ministre de la santé, a pris un arrêté afin de clarifier la situation, à savoir que désormais, « *Aucun transfert de données à caractère personnel ne peut être réalisé en dehors de l'Union européenne* »[616].

Une telle décision caractérise, une fois encore, la détermination négative des obligations liées à l'utilisation des données de santé. Il est question d'éviter tout risque de captation de données, donc promouvoir la protection et le respect de la vie privée des personnes concernées. En effet, un transfert des données de santé vers un hébergeur situé aux États-Unis aurait pu faire craindre que les données soient récoltées par des services de renseignements ou par des entreprises privées mal intentionnées. Il est plus sécurisant pour chaque pays et continent de récolter, d'utiliser et de garder, soit même, ses propres données, de telles pratiques n'évitant pourtant pas, à cent pour cent, les risques de fuite et de pillage de données[617].

---

614 CE., ord., 13 octobre 2020, n° 444937.

615 URL : https://www.cnil.fr//fr/la-plateforme-des-donnees-de-sante-health-data-hub

616 « *Après le deuxième alinéa du III de l'article 30 de l'arrêté du 10 juillet 2020 susvisé, il est inséré un alinéa ainsi rédigé : Aucun transfert de données à caractère personnel ne peut être réalisé en dehors de l'Union européenne* », Arrêté du 9 octobre 2020 modifiant l'arrêté du 10 juillet 2020 prescrivant les mesures générales nécessaires pour faire face à l'épidémie de covid-19 dans les territoires sortis de l'état d'urgence sanitaire et dans ceux où il a été prorogé.

617 I. Gavano et V. Le Marec, *Fuite massive de données personnelles de santé,* Dalloz actualité, 17 mars 2021 ; V. également, TJ Paris, ord. réf., 4 mars 2021, n° 21/51823.

L'interdiction de commercialisation des données personnelles et de transfert de celles-ci hors de l'Union européenne représentent les deux manifestations négatives les plus importantes. Les données de santé sont rares et précieuses, il convient, tant pour les individus que pour les organismes de santé, d'en garder la maitrise et la main mise.

218. Qu'en est-il maintenant en matière de relation de travail ? En effet, il a déjà été question, sur ce thème, de l'analyse de la détermination positive de l'utilisation des « données personnelles », à l'inverse qu'est ce qui n'est pas autorisé ?

Il convient, pour répondre à cette interrogation, de s'intéresser, d'une manière originale, à l'article du règlement européen qui traite spécifiquement du caractère licite du traitement de données personnelles. C'est ainsi qu'une lecture contraire de l'article 6 du règlement général sur la protection des données permet de mieux appréhender et comprendre ce qu'il faut entendre par détermination négative de l'utilisation des « données personnelles » dans la sphère du travail. En effet, chaque fois que le traitement, c'est à dire la collecte ou l'utilisation d'informations personnelles, ne sera pas en lien direct avec une relation de travail entre un employeur et son salarié, celui-ci sera non autorisé. En ce sens, le considérant 18 du Règlement général sur la protection des données personnelles permet une interprétation de ce qui n'est pas en lien direct avec une relation de travail entre un employeur et son salarié. Ce texte dispose en effet que « *Le présent règlement ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, et donc sans lien avec une activité professionnelle ou commerciale* »[618].

De ce fait, au sujet de la détermination négative de l'utilisation des données personnelles dans le cadre d'une relation de travail, le règlement en question propose deux axes de protection. D'une part, puisqu'il est imposé aux responsables de traitement, en l'occurrence les employeurs, de respecter plusieurs conditions bien définies, afin de se conformer au caractère licite du traitement, cela veut bien dire, à l'inverse, que dans le cas où une condition ne serait pas

[618] RGPD consid. 18, *préc.*

satisfaite, alors le traitement de données personnelles serait impossible car interdit. D'autre part, il est, également, question de protection des données personnelles des salariés et ce grâce à l'interdiction, ci-avant, énoncée. En effet, dans certains cas, si l'interdiction de traiter les données personnelles des employés existe c'est, *a contrario*, pour favoriser la liberté d'expression de ces derniers, dans le cadre d'activités strictement personnelles ou domestiques, comme c'est le cas par exemple pour l'échange de certaines correspondances ou pour l'utilisation de réseaux sociaux qui n'ont pas de lien avec une activité professionnelle ou commerciale. La frontière se situe donc entre d'un côté les activités professionnelles et de l'autre celles purement privées. C'est donc au sein de cette distinction qu'il convient d'appliquer la détermination positive ou négative de l'utilisation des « données personnelles », et ce au commencement du contrat de travail et jusqu'à son exécution.

219. Concrètement, au stade du recrutement, il est interdit pour un employeur de récolter des « données personnelles », auprès du candidat, alors qu'elles n'auraient aucun lien avec l'emploi en question. Par exemple, il ne sera pas possible pour l'employeur de demander au candidat son numéro de sécurité sociale, de lui demander des informations sur sa famille, ses opinions politiques ou religieuses, son appartenance syndicale ou encore son orientation sexuelle.

220. Au stade de la relation de travail, lorsqu'elle est établie et le salarié en poste, plusieurs dispositifs de contrôle utilisés par l'employeur sont à exclure. Si ces dispositifs sont à exclure c'est bien parce qu'ils portent essentiellement sur des « données personnelles » du salarié. A titre d'exemple, il sera interdit pour un employeur d'installer un dispositif de géolocalisation dans la voiture de son salarié si le but est seulement celui de contrôler le respect des conditions d'utilisation du véhicule par ce dernier (interdiction de contrôler le respect des limitations de vitesse) ou encore d'en contrôler en permanence les trajets (notamment les temps de pause, les temps de trajet pour se rendre ou aller à son domicile).

L'employeur ne pourra pas non plus utiliser de dispositif d'écoute ou d'enregistrement permanent ou systématique du salarié, ni même contrôler les

« données personnelles » d'un salarié stockées sur un ordinateur (c'est toute la question du secret autour des fichiers personnels du salarié).

Si par défaut, les fichiers présents sur l'outil informatique de l'entreprise, ont un caractère professionnel, l'employeur peut y accéder librement, toutefois certaines protections existent pour préserver la vie privée des employés. En effet, même sur son lieu de travail, un salarié a le droit au respect de sa vie privée, ce qui passe notamment par le respect et le secret dû à ses correspondances privées. Ainsi, il est impossible pour un employeur de consulter les courriels personnels des employés et ce même s'il a été fortement interdit, par le directeur d'entreprise, d'utiliser les ordinateurs de l'entreprise à des fins personnelles.
Attention toutefois, l'interdiction faite à l'employeur de ne pas consulter les messages personnels d'un salarié est contrebalancée par une obligation pour le salarié d'identifier spécifiquement la nature de ces derniers. Ainsi, pour se protéger de toute intrusion, il ne suffira pas d'insérer un courrier personnel dans un dossier nommé par les initiales de l'employé, il faudra stocker ces derniers dans un répertoire dont l'intitulé reprend la mention « Personnel » ou « Privé »[619].

Une autre situation, anodine, permet de démontrer que le rôle de l'employeur à l'égard des données personnelles de ses salariés n'est pas sans limite. Toujours liée à l'actualité et à la crise sanitaire, une clarification s'est imposée quant à la prise de température des salariés.
En effet, afin d'éviter la multiplication de contamination liée à la maladie de Covid19, au sein de l'entreprise, certains employeurs avaient décidé de prendre et de tester la température de leurs salariés.
Si la prise de température manuelle est tolérée, par mesure de précaution, cette procédure doit être organisée et mise en œuvre dans le cadre de l'élaboration de notes de service valant adjonction au règlement intérieur comme le précise l'article L. 1321-5 du Code du travail[620]. En tout état de cause, si la prise de

[619] URL : https://www.cnil.fr/sites/default/files/atoms/files/travail-vie_privee.pdf

[620] « *Les notes de services ou tout autre document comportant des obligations générales et permanentes dans les matières mentionnées aux articles L. 1321-1 et L. 1321-2 sont, lorsqu'il existe un règlement intérieur, considérées comme des adjonctions à celui-ci. Ils sont, en tout hypothèse, soumis aux dispositions du présent titre. Toutefois, lorsque l'urgence le justifie, les obligations relatives à la santé et à la sécurité peuvent recevoir application immédiate. Dans ce cas, ces prescriptions sont immédiatement et*

température des salariés est autorisée, elle n'est pour autant pas recommandée ni par le Ministère du travail[621], ni par le Haut conseil de santé publique[622], à savoir qu'un tel procédé n'est pas toujours fiable et efficace, pour ce type de situations, un relevé de température élevé ne résultant pas nécessairement du Covid19.
S'il est possible pour l'employeur d'une part de demander à ses salariés de prendre, eux même, leur température chez eux, d'autre part de tester ces derniers manuellement en entreprise, il est, à l'inverse, formellement, interdit de réaliser des contrôles de températures par des moyens automatiques. En effet, il est interdit aux employeurs de mettre en place des outils obligatoires de captation automatique de température (telle que des caméras thermiques)[623].

Derrière cette interdiction, la volonté est d'éviter toute constitution de fichiers sur les salariés, leurs santés, ce qui reviendrait à ne pas respecter leurs données personnelles, constituant une atteinte à leur vie privée. C'est donc la nuance autour de la question de constitution de fichier qui permet d'autoriser ou non la prise de température. Lorsque ce procédé est réalisé manuellement, il n'y a aucune trace donc aucune atteinte. En revanche, de manière automatisée, c'est-à-dire avec des outils pour tester et d'autres pour prendre les résultats, il est, forcément, question de constitution de fichier. Même si l'employeur est de bonne foi et qu'il ne réalise pas de fichiers à proprement parler, l'outil technologique et informatique utilisé enregistrera en mémoire les tests, ce qui correspond à la réalisation de fichiers.

Afin d'éviter toutes atteintes à la vie privée des salariés, ce qui est le critère permettant ou non l'utilisation par l'employeur de données personnelles dans l'entreprise, l'alternative la plus responsable est, quand cela est possible, le télétravail.

---

simultanément communiquées au secrétaire du comité social et économique ainsi qu'à l'inspection du travail », C. trav., art. L. 1321-5.

[621] Protocole national pour assurer la santé et la sécurité des salariés en entreprise face à l'épidémie de Covid-19, 31 aout 2020.

[622] Avis du Haut Conseil de la santé publique relatif à un contrôle d'accès par prise de température dans la préparation de la phase de déconfinement en lien avec l'épidémie à Covid-19, 28 avril 2020.

[623] URL : https://www.cnil.fr//fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-données-personnelles-par-les-employeurs

221. La détermination négative des obligations liées à l'utilisation des données personnelles au sein d'un contrat de travail est simple, chaque fois qu'un traitement s'intéresse à une donnée personnelle alors que cela ne concerne que la vie privée du salarié et pas la relation de travail, ce dernier est interdit. L'utilisation de données personnelles n'est donc possible que si cela est justifié pour l'intérêt de l'entreprise. Le salarié est donc un acteur protégé du monde du travail, ses données ne peuvent être récoltées, utilisées, qu'à des conditions très strictes. Cet encadrement est favorable pour l'employeur, ce dernier, en prenant certaines précautions, installe une relation de confiance avec ses employés qui ne se sentent ni soumis, ni espionnés et peuvent, de ce fait, pleinement s'investir dans leur travail.

Section 2 : Les modalités de l'utilisation de la donnée personnelle

222. S'intéresser aux différentes modalités propres à l'utilisation de la donnée personnelle revient à s'intéresser au cadre général du consensus entre les parties au contrat (Paragraphe 1) et au cadre spécifique existant au-delà du contrat (Paragraphe 2).

§1 Le cadre général du consensus entre les parties au contrat

223. Juridiquement, le consentement s'entend comme une « *manifestation de volonté par laquelle une personne s'engage dans un acte juridique* »[624]. Le consentement requis est donc, comme cela a été plusieurs fois évoqué, primordial en matière de « données personnelles ». En effet, sans cette autorisation ou approbation donnée par la personne concernée, le responsable de traitement ne pourrait ni collecter, ni utiliser les informations personnelles en question.

C'est à ce titre que l'article 6 du règlement général sur la protection des données encadre la licéité du traitement en imposant la règle qui suit, à savoir que « *Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques* »[625].

224. Si un responsable de traitement peut, aisément, collecter et utiliser les « données personnelles » d'une personne à des fins et en adéquation avec ce qui a été voulu et accepté par la personne concernée, peut-il en jouir autrement ?

Se pose ici la question de la transmissibilité des données à caractère personnel. Les « données personnelles », obtenues avec l'accord de le personne concernée, sont-elles cessibles, transmissibles ou encore négociables ? En d'autres termes,

---

[624] Dictionnaire du vocabulaire juridique 2019, *Op cit.*

[625] RGPD art. 6, *préc.*

ces données sont-elles aliénables ? S'il convient de répondre à ces différentes interrogations par la négative, en voici les explications.

L'inaliénabilité est entendue droit civil comme la « *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* »[626].

Tel que cela ressort des analyses précédentes[627], la notion de « donnée personnelle » est étroitement liée avec celles de l'honneur ou encore de la dignité humaine. Ces caractéristiques fondent les droits fondamentaux et inaliénables inhérents à la personne humaine.

En effet, les droits de la personnalité sont les droits qui assurent à l'individu la protection des attributs de sa personnalité tels que la vie privée, l'image ou encore la voix et permettent ainsi d'en garantir son intégrité morale.

Les données à caractère personnel font donc intégralement partie du droit de la personnalité et par conséquent, leur caractère inaliénable est incontestable. C'est en effet ce qui se dégage à la lumière de l'article 16-1 du Code civil, notamment à l'alinéa 3, ce dernier déclarant à ce titre que « *Le corps humain, ses éléments et ses produits ne peuvent faire l'objet d'un droit patrimonial* »[628].

Si d'un côté, la loi relative à l'informatique, aux fichiers et aux libertés, dans sa version originelle du 6 janvier 1978 protège les différentes offenses faites aux « données personnelles » en affirmant en son article 1er que « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. 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* »[629], de l'autre, le Code civil s'efforce de garantir l'aspect non

---

626 Lexique des termes juridiques, *préc.*

627 *V. supra §n°9, 70 et 81.*

628 « *Chacun a droit au respect de son corps. Le corps humain est inviolable. Le corps humain, ses éléments et ses produits ne peuvent faire l'objet d'un droit patrimonial »*, C. civ., art. 16-1.

629 Art. 1er, Loi n°78-17 du 6 janvier 1978, *préc.*

négociable, incessible et encore intransmissible des données à caractère personnel.

Bien heureuse en est la conséquence ! En effet, imaginer que les « données personnelles » puissent avoir un caractère aliénable reviendrait à ouvrir la boite de Pandore, tant les hypothèses préjudiciables, pour ces dernières et pour leurs titulaires, paraissent infinies.

225. Le règlement général sur la protection des données interdit aux responsables de traitement de procéder à la commercialisation des « données personnelles », il ne faut pas que cette interdiction soit levée lorsque celui qui souhaite vendre les « données personnelles » en est le titulaire. Accepter une telle manœuvre reviendrait à remettre en cause le principe d'inaliénabilité qui touche aux droits de la personnalité.

Une atténuation des propos précédents est possible : en effet, certaines catégories, les « tiers autorisés », disposent de l'autorité nécessaire, parce que légalement conférée, pour exiger des organismes la transmission de documents ou de renseignements pouvant comprendre des données personnelles.
Il faut entendre par « tiers autorisé »[630] toute entité, structure, organisation, le plus généralement des autorités publiques ou des auxiliaires de justice qui, en vertu de la loi, sont autorisées à recueillir par demande des données personnelles, elles-mêmes contenues dans des fichiers publics et privés. A titre d'illustration[631], ont la qualité de tiers autorisés, l'administration fiscale, les organismes de sécurité sociale (dans le cadre de la lutte contre la fraude) et les organismes en charge de l'instruction, du versement et du contrôle du revenu de solidarité active, les administrations de la justice, de la police et de la gendarmerie ou encore les huissiers de justice.

---

[630] « *Une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel* », RGPD art. 4 (10.), *préc.*

[631] URL : https://www.cnil.fr/fr/cnil-direct/question/quest-ce-quun-tiers-autorise

Si la transmission de données personnelles semble, limitée, mais pour le moins possible, comment se manifeste-t-elle en pratique ? Le caractère intime et sensible des données personnelles est-il toujours respecté malgré une pareille autorisation ? Plusieurs étapes façonnent et renforcent la procédure de transmission des données aux tiers autorisés.

Lorsqu'une demande de transmission de donnée est réalisée, il convient, en premier lieu, de vérifier le fondement légal de cette dernière. Sans référence ou fondement légal et réglementaire, aucune requête ne peut aboutir, les tiers n'étant habilités et autorisés, pour de telles démarches, qu'en vertu de la loi. Ensuite, il est primordial de vérifier la qualité du tiers à l'origine de ladite demande, sans cette qualité le tiers ne serait pas autorisé et n'aurait donc pas droit à obtenir de telles informations. Enfin, il convient de s'assurer de la sécurité des mesures de communications, si tel n'est pas le cas, le risque engendré pour les données conduirait au refus de la demande initiale de transmission des données.

Soucieuse des conséquences que pouvait engendrer la transmission des données personnelles, la Commission de l'informatique et des libertés a réalisé un guide pratique[632] autour de la notion de « tiers autorisés » afin de clarifier une telle manœuvre, preuve, une fois de plus, de la vigilance accordée à la protection des données. Cette documentation fait la démonstration de diverses situations démontrant la validité ou non de demande de transmission de données. Par exemple, un refus est possible, même si un texte légal est visé, lorsque la portée de celui-ci est trop large. A l'inverse, la transmission de données sera valide et accordée lorsque l'organisme placé en tant que tiers autorisé fonde sa demande sur des dispositions précises, ce qui sécurise l'échange en question.

Si la transmission de données à des tiers est possible, celle-ci est marginale, spécifique et surtout très encadrée. Les organismes autorisés à demander de tels agissements sont peu nombreux et sont soumis, par souci de confiance, à une approbation légale ou réglementaire. Le risque pour les données personnelles est dans ce cas d'espèce réduit, les vérifications du procédé de transmission étant multiples et strictes. Il ne faut, cependant, pas oublier que le principe reste

[632] URL : https://www.cnil.fr/sites/default/files/atoms/files/guide_tiers_autorises.pdf

l'inaliénabilité et l'intransmissibilité des données, l'exception étant les rares possibilités offertes aux tiers autorisés. En effet, si les tiers autorisés sont une exception en ce qu'ils peuvent, sous plusieurs conditions, jouir d'une certaine liberté pour la transmission de données personnelles, cette possibilité n'a pas vocation à se développer et se cantonne donc pour ces organismes bien spécifiques.

226. D'une manière générale, l'utilisation des données personnelles est soumise aux principes d'inaliénabilité et d'intransmissibilité des données personnelles dont la finalité est celle de s'opposer à toute marchandisation et commercialisation des données personnelles, ce qui serait un fléau pour les données mêmes, mais aussi et surtout pour les personnes concernées. En définitive, lorsqu'un responsable de traitement est autorisé à collecter et utiliser les données personnelles d'une personne concernée, dans le cas de figure où celle-ci a consenti en ce sens, il ne dispose pas de liberté dans cette manœuvre, c'est-à-dire qu'il ne peut pas outrepasser le consentement de la personne puisque c'est cela qui conditionne le traitement de données en question. En effet, l'utilisation des données personnelles par le responsable de traitement est encadrée par des modalités voulues par les parties, voilà pourquoi celui-ci ne peut en disposer librement.

L'inaliénabilité des « données personnelles » ne fait plus aucun doute, toutefois une autre question se présente, celle de savoir si le titulaire de « données personnelles » détient l'usus, le fructus et l'abusus de ces dernières ? En d'autres termes, la personne concernée au sens du Règlement européen sur la protection des données est-elle propriétaire de ses « données personnelles » ?

Là encore, la réponse se forme par la négative. Si dans le sens courant le titulaire de la donnée à caractère personnel est imaginé comme étant propriétaire de celles-ci, en réalité en pratique, il n'en est rien.

227. Le droit de propriété est l'un des droits français les plus sacrés. Il offre la possibilité d'user, de profiter et de disposer d'une chose, d'en être le maitre absolu. L'article 544 du Code civil, précise en ces termes que « *La propriété est*

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 »[633].

Si la question de la propriété des données personnelles par les personnes concernées se pose, c'est en partie en raison de la Cour de cassation. En effet, cette dernière, dans un souci de protection des données, a d'abord créé, puis affirmé, sur ce point, une situation juridique ambiguë.

Par le célèbre arrêt « Bluetooff »[634], les hauts magistrats de la chambre ont, pour la première fois, considéré explicitement qu'une donnée numérique pouvait faire l'objet d'une soustraction frauduleuse. Le vol par téléchargement de données numériques était donc né. Pour autant, si la Cour de cassation considère que l'infraction de vol[635] est constituée, ce qui semble contraire avec l'infraction en question[636], la chambre criminelle justifie sa position par le fait que le prévenu s'est rendu coupable de s'être introduit dans un système de traitement automatisé, d'avoir téléchargé des données et enfin de les avoir utilisées. Tous ces éléments réunis caractérisent et déterminent la soustraction frauduleuse de données informatiques.

Deux années plus tard, voilà que la (quasi-)consécration du vol d'informations était réaffirmée par un arrêt en date du 28 juin 2017[637], la Cour de cassation mesurant toutefois ces propos par l'emploi, cette fois, pour caractériser l'infraction, du terme « d'appropriation frauduleuse » des données.

Si le rapprochement entre la notion de vol et celle de donnée représente pour celle-ci une sécurité supplémentaire, la portée d'une telle nouveauté ne semble pas

---

633 C. civ., art. 544.

634 Cass. crim., 20 mai 2015, 14-81.336, *Bull. crim.* 2015, n°119 ; *D* 2015, p. 1466, note L. Saenko ; *JCP* 2015, éd G., II, 887, note G. Beaussonie ; *Gaz. Pal.* 2015, 1 p.8, note S. Detraz ; *Dr. pénal* 2015, comm. 123, note P. Conte.

635 « *Le vol est la soustraction frauduleuse de la chose d'autrui* », C. pén., art. 311-1.

636 « *La soustraction étant le fait d'ôter, de soustraire (au sens mathématique, presque), elle induit une perte du côté de la victime, et un gain de celui de l'auteur. Soit une conséquence patrimoniale invérifiable si l'objet de la soustraction est une information – laquelle continuera, même après sa soustraction, à bénéficier à son propriétaire. Quant à l'objet de la soustraction, la loi vise expressément une chose* », L. Saenko, *La (quasi-) consécration du vol d'informations*, RTD com., Revue trimestrielle de droit commercial et de droit économique, Dalloz, 2017, pp. 713.

637 Cass. crim., 28 juin 2017, 16-81.113, Publié au bulletin *(P+B)*.

encore s'inscrire dans la durée[638]. En effet, tant en droit pénal qu'en droit des biens, l'émergence de cette caractérisation semble confuse.

La Cour de cassation ayant développé le vol, la soustraction ou même l'appropriation de données, est-ce à dire qu'il existe un véritable droit de propriété des données personnelles ?

Cette hypothèse est en tout cas défendue par certains partisans qui évoquent l'idée d'un droit de propriété des données et justifient cela par la valeur économique de celles-ci. Pour ces derniers, si la donnée personnelle a une valeur économique, il faut alors la considérer comme un bien à part entière, il parait, alors à ce titre, nécessaire de la protéger. Selon cette pensée, reconnaitre un droit de propriété des données personnelles permettrait deux conséquences positives : d'une part, cela reviendrait à restaurer la maitrise, la mainmise des personnes concernées sur leurs données et de l'autre cela permettrait, à ces dernières, de profiter des avantages et bénéficies liés à leur exploitation.

Si le premier argument justifiant la création d'un tel droit de propriété sur les données est louable, le second en revanche fait craindre le pire. Le principe d'interdiction de commercialisation des données doit perdurer. En justifiant la création d'un droit de propriété des données par une position économique, le combat semble perdu d'avance. Il n'est pas concevable de promouvoir l'idée d'un droit de propriété pour favoriser la protection des données personnelles tout en introduisant celles-ci dans une démarche de monétisation. Procéder à un tel bouleversement reviendrait en réalité à renforcer les déséquilibres entre les personnes concernées par les données personnelles et les responsables de traitement, entendus au sens des géants du numérique. Si l'hypothèse d'un droit de propriété des données était réelle, les personnes concernées seraient soumises par les puissants, eux qui useraient de leurs positions dominantes pour soutirer et collecter en plus grandes quantités des informations pour en tirer profit.

---

[638] « *Sans doute la reconnaissance officielle du vol d'informations est-elle pour bientôt. Peut être sous la forme d'un attendu de principe qui, à défaut de modification législative, stipulerait qu'une information constitue une chose au sens de l'article 311-1 du code pénal. Seul l'avenir, encore, le dira »,* L. Saenko, *La (quasi-) consécration du vol d'informations, Op cit,* pp. 713.

La création d'un droit de propriété serait également un non-sens dans nombre de situations, il faut imaginer, par exemple, qu'une personne autorise un responsable de traitement à utiliser ses données et ensuite décide de vendre l'intégralité de ses informations personnelles à un autre responsable. Il y aurait, alors, une situation inédite dans lequel le premier traitement serait nul puisque sans objet. Pire encore, en développant l'exemple précédent, peut-on réellement imaginer qu'une personne vende l'intégralité de ses données ? Une personne peut-elle valablement se retrouver dépossédée de l'intégralité de ses informations ? La réponse est bien entendu négative, il serait bien étonnant qu'une personne s'accapare pour elle-même de son numéro de sécurité sociale ou de son état civil pour le vendre à quelqu'un d'autre.

228. A défaut de pouvoir conférer aux personnes concernées un réel droit de propriété des données personnelles, ces dernières peuvent toutefois se prévaloir d'une maitrise[639] de celles-ci.

La personne concernée n'est en réalité jamais complètement dépossédée de ses données, elle dispose d'un droit de suite, d'un droit de regard, sur le traitement réalisé. Le responsable de traitement est tenu, par diverses conditions et restrictions, de respecter les données personnelles.

Comme en matière contractuelle, un consensus existe entre les parties. Si la personne concernée donne son consentement au traitement des informations les plus précieuses qu'elle dispose, *a contrario* le responsable de traitement est tenu par ses engagements et doit, puisqu'il profite de ces données, veiller sur elles.

229. Aussi, comme cela a été évoqué précédemment, les « données personnelles » ne sont que des attributs de la personnalité, le titulaire ne peut pas en disposer comme il l'entend. Il lui est en effet interdit de les aliéner. Ceci explique que le droit de propriété ne s'intéresse pas aux « données personnelles », et l'inverse serait dangereux puisqu'encore une fois cela irait à l'encontre du principe d'inaliénabilité qui touche aux droits de la personnalité.

---

[639] RGPD art. 20, *préc.*

§ 2 Le cadre spécifique au-delà du contrat

230. Au-delà de ce cadre général et conventionnel, il y a des modalités particulières qui peuvent être rendues nécessaires dans certains domaines.

Là encore, le domaine de la santé en fournit une illustration intéressante. Les autorités sanitaires s'accordent[640] sur le fait que le principe de base de la protection des données de santé à caractère personnel repose sur la responsabilisation des opérateurs et de leurs sous-traitants. C'est à dire sur la responsabilisation des contractants, comme cela vient d'être vu.

Ainsi, les établissements sanitaires et médico-sociaux d'une part, les acteurs institutionnels, les industriels pharmaceutiques et du dispositif médical, d'autre part voire même les start-up en santé, etc. sont-ils tenus dans leurs rapports contractuels de respecter et de faire respecter le champ dégagé par le Règlement général sur la protection des données.

231. Mais par-delà de ce devoir contractuel, ceux-ci doivent respecter de nouvelles obligations, lesquelles font référence à l'émergence du principe de responsabilité[641] également appelé principe d'*accountability*[642], nouveauté introduite par le règlement général sur la protection des données.

Concrètement, le règlement européen impose au responsable de traitement, de prendre toutes les mesures nécessaires afin que le traitement des données en question respecte son application et soit en mesure de le prouver. Il s'agit ici d'une avancée majeure pour les personnes concernées, la sécurité de leurs données devant être assurée par la personne qui utilise ces dernières. Bien plus que de simplement rappeler aux responsables de traitement qu'ils doivent collecter et

---

640 V. *La Gazette de la santé*, numéro spécial, 2 octobre 2018 : URL : http://www.gazette-sante-social.fr/48652/la-protection-des-donnees-de-sante-apres-le-rgpd

641 *V. supra §n°54.*

642 « *L'accountability (principe issu de l'article 5 du RGPD) désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données* », URL : https://www.cnil.fr/fr/definition/accountability

traiter les données personnelles des personnes concernées en respectant les règles édictées, le règlement européen fait peser sur ces derniers la charge de la preuve de ce respect, ce qui est gage de sécurité. De plus, ce principe est l'occasion pour les responsables de traitement, plus que de seulement réparer le dommage, d'anticiper les difficultés que pourrait rencontrer le traitement de données. Voilà qu'en dégageant une obligation double, ce principe d'*accountability* renforce la protection des données.

232. D'une manière générale, en pratique, l'*accountability* est symbolisée par la rédaction de plusieurs documents attestant des mesures mises en place afin de démontrer que le traitement des données en question est adéquat[643]. L'obligation consistant pour les responsables de traitement de rendre des comptes s'inscrit pleinement dans l'intérêt des données de santé et des patients. En effet, les données de santé ont par nature un caractère intime, il est de ce fait logique qu'une telle mesure soit prise pour renforcer leur sécurité.

Pour s'assurer de la bonne exécution du principe d'*accountability*, l'une des premières étapes concerne la nomination obligatoire d'un délégué à la protection des données[644], notamment, en cas de traitement à grande échelle, en l'espèce ce qui est le cas pour les données de santé. Ce délégué prendra, au vu des nouvelles dispositions, le relais des précédents correspondants informatique et libertés.

Soumis à une obligation de confidentialité, le délégué à la protection des données devra veiller à l'application du Règlement européen et conseiller l'établissement de santé ou son partenaire contractuel sur les sujets relatifs à la protection des données de santé recueillies par celui-ci[645]. A ce titre, le délégué à la protection des données, gardien de la conformité du règlement européen, sera l'interlocuteur privilégié de la Commission nationale de l'informatique et des libertés [646] et pourra pour ce faire s'appuyer sur un dossier d'*accountability*.

---

643 URL : https://www.village-justice.com/articles/accountability-rgpd-liste-des-documents-contenus-dans-dossier-conformite,33433.html

644 RGPD art. 37, *préc.*

645 RGPD art. 38 et 39, *préc.*

646 RGPD art. 39 (1.e), *préc.*

233. Aussi, toujours dans le champ sanitaire en exemple, il sera mis en place un registre[647] interne aux établissements qui détiennent des données de santé, permettant de rendre compte de la conformité du traitement au règlement européen. Si l'utilisation d'un tel registre n'est pas obligatoire, il s'impose pour les entreprises ou organisations de plus de 250 personnes, sauf si le traitement effectué par ces dernières est susceptible de comporter des risques pour le droits et libertés des personnes concernées, ce qui sera nécessairement le cas en matière de santé.

Le registre de traitement mis en place devra mentionner notamment le nom et les coordonnées de l'entreprise responsable du traitement et du délégué à la protection des données, les finalités du traitement, la description des catégories des personnes concernées, les délais prévus pour l'effacement des données, la description des mesures de sécurité pour les protéger, et devra être transmis à la Commission nationale de l'informatique et des libertés en cas de contrôle.

S'il peut être interprété, négativement, comme un moyen de contrôle de la conformité des traitements réalisés, la mise en œuvre d'un registre de traitement peut, positivement, être le moyen, pour les responsables de traitement, de vérifier que leurs activités de traitement sont conformes aux attentes. Il apparait que ce moyen permet plus d'inciter les responsables de traitement à se conformer au règlement général sur la protection des données plutôt que de les sanctionner pour le non-respect de celui-ci. L'obligation de tenue d'un registre est un procédé, en apparence, non coercitif permettant aux responsables de traitement de se soumettre au principe d'a*ccountability*.

234. En outre, en raison de la conséquence, déjà évoquée, sur les droits et libertés fondamentaux des individus ainsi que de la portée générale et absolue du secret médical, tout opérateur doit sécuriser les traitements de données de santé. S'il va de soi que le professionnel contractant devra, mettre en œuvre des processus garantissant la sécurité et la confidentialité des données et le respect des

[647] RGPD art. 30, *préc.*

droits des personnes (clauses contractuelles, procédures internes…)[648], le règlement européen sur la protection des données lui impose d'autres mesures.

Il doit ainsi réaliser une analyse d'impact[649] préalable portant sur les risques techniques de sécurité et les risques juridiques pour la vie privée des personnes concernées. Cette analyse contient une description des opérations de traitement et la finalité poursuivie, une évaluation de l'intérêt au regard des risques, et une évaluation sur les mesures de protection mises en place pour limiter le risque (anonymisation, certificat SSL, cryptage des données…).

Si l'obligation de mener une analyse d'impact n'est pas obligatoire pour les professionnels de santé, notamment lorsque ces derniers exercent à titre individuel, cette exigence est, toutefois, nécessaire si l'exercice professionnel se fait au sein, d'un réseau, d'une maison de santé, ou encore, d'un centre de santé. En définitive, à chaque fois qu'en raison de l'activité, les données personnelles, en l'espèce les données de santé, sont susceptibles d'être partagées avec d'autres professionnels de santé, alors, une analyse d'impact sera obligatoire. Une nouvelle fois, la logique du règlement européen de protection des données est celle de protéger les données, il est de ce fait normal qu'une telle obligation s'impose quand les données de santé ont vocation à être partagées entre plusieurs professionnels.

A l'inverse, dans le cas de figure présenté en amont, lorsqu'un médecin exerce, par exemple, tout seul, l'intérêt qu'il réalise une analyse d'impact n'a peu ou pas d'intérêt, puisqu' il n'y a pas de réel risque pour les données de santé. En effet, l'obligation de réaliser une analyse d'impact des données dans le secteur de la santé s'impose dès lors que le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Ce cas de figure se retrouve, naturellement, lorsque le traitement est réalisé à grande échelle et qu'il concerne des catégories particulières de données. Ainsi, il n'est pas anormal de ne

---

[648] *V. supra §n°46, 146 et 206.*

[649] « *Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel* »,RGPD art. 35 (1.), *préc.*

pas soumettre une pareille obligation lorsque le responsable de traitement est un professionnel de santé qui exerce à titre individuel. L'un des plus grands dangers pour les données de santé étant celui de la transmission des données avec la crainte que celles-ci soient captées et réutilisées à des fins non conformes à leur usage originel, la distinction est donc aisée à comprendre : quand un traitement de données implique plusieurs professionnels de santé, une analyse d'impact est obligatoire, tandis que si ce traitement est réalisé par un professionnel seul, une telle analyse est facultative.

235. Le Règlement sur la protection des données oblige enfin à signaler[650] à la personne concernée, c'est-à-dire le patient, tout incident de sécurité impliquant ses données personnelles, obligation également prévue, en terme similaire, en matière de santé[651].

Ce dispositif de sécurité, basé sur un système de signalement, incombe, selon le Code de santé publique, aux établissements de santé, mais aussi aux organismes et services de santé, en qualité de responsables de traitement, d'avertir dans les plus brefs délais l'Agence régionale de santé concernant les incidents grave de sécurité à l'encontre des systèmes d'information. Si le règlement européen impose un signalement analogue, il limite toutefois la portée de celui-ci puisqu'il intéresse seulement la personne concernée. En définitive, il semble que le règlement européen pose le principe général propre au signalement en cas d'atteinte aux données personnelles et que le Code de la santé publique précise celui-ci en rajoutant des conditions.

Tant par le règlement UE 2016/679 que par le Code de la santé publique, la donnée de santé est, parce que sa nature l'impose, surprotégée.

236. Malgré la diversité des mesures mises en place par le règlement européen sur la protection des données, pouvant entrainer une certaine confusion, il

---

650 « *Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais* », RGPD art. 34 (1.), *préc.*

651 « *Les établissements de santé et les organismes et services exerçant des activités de prévention, de diagnostic ou de soins signalent sans délai à l'agence régionale de santé les incidents graves de sécurité des systèmes d'information.* », CSP., art. L. 1111-8-2.

convient de vanter les mérites de ce dernier. En effet, il semble qu'à chaque étape du traitement de données personnelles correspond une obligation pour le responsable de traitement, ce qui représente, pour la personne concernée et ses données, un gage de sécurité et de confiance. Il semble que l'une des forces du règlement général est le fait de ne rien avoir laissé au hasard, lui qui encourage l'élaboration d'un Code de conduite[652] et ce pour chaque secteur de traitement. Un tel ouvrage est en préparation, dans le domaine de la santé, son but serait « *d'apporter des réponses pragmatiques et faciles d'accès* »[653].

En matière de santé, si la protection des données de santé est déjà assurée par le Code de la santé publique, le règlement général sur la protection des données a élaboré diverses conditions pour compléter cette démarche relative à la sécurité de celles-ci. Toutes les phases présentées, en amont, découlent du principe d'*accountability* et sont nécessaires en matière de santé, mais également pour d'autres domaines, chaque fois que le traitement peut avoir des risques avérés pour les données personnelles.

237. En tant que données dites sensibles, les données de santé bénéficient d'une protection toute particulière. A ce sujet, si les règlementations en vigueur imposent, aux responsables de traitement, la mise en œuvre de formalités préalables afin de justifier de la bonne utilisation desdites données, ce qui émane, notamment, du principe de transparence, le règlement européen de protection des données personnelles a changé cette manière de fonctionner. En effet, en consacrant le principe d'*accountability*, ci-dessus énoncé, le règlement en question a choisi de sécuriser les données de santé en responsabilisant les acteurs, c'est-à-dire les responsables de traitement. Concrètement, l'idée est celle d'abandonner le mécanisme de formalités préalable et celui de contrôle *a priori* des autorités de contrôle pour laisser place à un mécanisme d'autocontrôle

---

652 « *Les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises. Les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent élaborer des codes de conduite, les modifier ou les proroger, aux fins de préciser les modalités d'application du présent règlement* », RGPD art. 40, *préc.*

653 URL: https://escaramozzino.legal/2019/05/29/rgpd-sante/

conjugué par un contrôle *a posteriori* des autorités. Une fois encore, il faut remarquer que les règles édictées, en matière de santé, sont soit complétées, soit modifiées, si besoin, soit remplacées, lorsque cela est nécessaire, mais ce, toujours, dans l'intérêt des données de santé. Ainsi, si le présent règlement apporte de la nouveauté, pour accroitre la protection des données, à travers des modalités particulières, il s'appuie, néanmoins, sur des bases préexistantes.

C'est donc ici un exemple intéressant de ce qui peut être fait au-delà du pur cadre contractuel et l'influence que le Règlement UE 2016/679 peut avoir sur le contrat, car ces obligations s'ajoutent aux règles édictées par le Code de la santé publique et relatives à l'hébergement externalisé des données de santé couvertes par le secret médical, à la pratique de la télémédecine, à l'identifiant national de santé, etc.

238. Il est aisé de comprendre que ce nouveau cadre juridique garantit au citoyen la sécurité maximale de ses « données personnelles », la transparence de leur traitement et le respect de ses droits.

CONCLUSION DU CHAPITRE 1

Lorsque l'exécution d'un contrat est en lien avec l'utilisation de la donnée personnelle, la singularité de cette notion implique des obligations aux finalités tant positives que négatives, mais impose également certaines modalités particulières.

Chapitre 2 : Les obligations liées à la protection de la donnée personnelle

239. Deux types d'obligations ont pour but la protection de la donnée personnelle : il s'agit, en premier, de l'obligation de confidentialité (Section 1) et, ensuite, de l'obligation de protection et de conservation des données personnelles (Section 2).

Section 1 : Les données personnelles et les obligations de confidentialité

240. L'obligation de confidentialité propre aux données personnelles s'étudie par le caractère contractuel de l'obligation de confidentialité à l'égard de la donnée (Paragraphe 1) et par le caractère universel de l'obligation de secret à l'égard de la donnée (Paragraphe 2).

§1 Le caractère contractuel de l'obligation de confidentialité à l'égard de la donnée personnelle

241. Il convient, tout d'abord, de présenter l'obligation de confidentialité et de la confronter aux données personnelles (A), pour ensuite s'intéresser à cette obligation, en pratique, par l'exemple du contrat de travail (B).

A) Présentation et confrontation de l'obligation de confidentialité à l'égard de la donnée personnelle

242. La donnée sensible forme une catégorie particulière de « donnée personnelle »[654], information si délicate et si spécifique, pour celui qui consent à la divulguer, qu'elle doit, à ce titre, bénéficier d'une attention et d'une protection toute singulière.

Sans se contenter de refuser simplement et catégoriquement le traitement de ces données spéciales, excepté certaines exceptions déterminées[655], il est question, lorsque l'utilisation de celles-ci est autorisée, d'imposer certaines réserves.

---

654 « *Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* », URL : https://www.cnil.fr/fr/definition/donnee-sensible

655 « *1. Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou*

A ce sujet, Nicolas Dissaux donne un élément de réponse et prétend que « *Souvent, lorsque la négociation implique l'échange d'informations sensibles, voire les éléments d'un savoir-faire, les parties stipulent un engagement de confidentialité* »[656]. L'engagement ou accord de confidentialité est donc l'outil privilégié pour astreindre les différents interlocuteurs d'un contrat de respecter le caractère confidentiel des informations communiquées, ce qui en limite considérablement leur usage.

Pour ce faire, le Code civil prévoit à l'article 1112-2 que « *Celui qui utilise ou divulgue sans autorisation une information confidentielle obtenue à l'occasion des négociations engage sa responsabilité dans les conditions du droit commun* »[657].

Ainsi par cette disposition, le Code civil affirme l'obligation de confidentialité en vue de protéger une partie faible, en l'occurrence le titulaire qui consent à divulguer les « données personnelles » le concernant.

Au regard de cet article, il est donc fait obligation pour le responsable du traitement de respecter le caractère confidentiel des « données personnelles », tant dans leur utilisation que pour leur divulgation. Cette obligation de confidentialité n'est pas à prendre à la légère, en effet, au regard du texte, elle engage la responsabilité de la partie qui utiliserait ou divulguerait l'information confidentielle en violation de cette obligation.

Outre le fait que la confidentialité évoque principalement un risque de sanction, pour la personne qui y contreviendrait, en outrepassant cette obligation, il ne faut pas oublier que cette faculté est également utilisée pour sensibiliser et informer les personnes sur l'importance des informations et données en question, mais également sur les conséquences d'une divulgation.

---

l'orientation sexuelle d'une personne physique sont interdits. 2. Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie (...) », RGPD art. 9 (1.,2.), *préc.*

656 N. Dissaux, *Contrat : formation – Détermination des conditions, Op. cit.*

657 C. civ., art. 1112-2 *(Ord. nº 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

243. Appliqué aux « données personnelles », il convient de se demander quelle est l'utilité des clauses de confidentialité et comment leur validité est-elle gouvernée ?

L'obligation de confidentialité est, par principe, convenue durant les négociations précontractuelles, le plus souvent, elle émane d'une clause insérée dans un accord préparatoire ou d'un accord autonome de confidentialité. Puisque c'est un accord qui permet de faire naitre l'obligation de confidentialité, cela démontre que celle-ci est, nécessairement, voulue par les parties, d'une part, pour se protéger l'une de l'autre, mais aussi et surtout, d'autre part, pour protéger l'objet sur lequel elle porte, à savoir les informations échangées, c'est-à-dire en l'espèce les données personnelles.

Outre la question du formalisme de cette obligation, lequel démontre néanmoins que cette dernière lie les parties dans un intérêt commun à savoir la protection des données personnelles, en s'intéressant au fond de l'obligation de confidentialité, il est possible de remarquer que celui-ci dispose d'un objectif double[658], démontrant, une nouvelle fois, l'importance pour les données personnelles d'un tel accord. Selon Magali Jouen, « *En attirant l'attention des parties sur l'importance et la valeur attachées à certaines informations échangées au cours des négociations, ils peuvent tout d'abord jouer un rôle pédagogique et préventif. En permettant aux parties de se doter d'une protection ciblée et « sur mesure », ils remplissent ensuite une fonction complétive* »[659]. L'obligation ne vise donc pas seulement à protéger la partie faible (la personne concernée titulaire d'une « donnée personnelle » par exemple), même si cet objectif est légitime et naturel, mais vise également à attirer l'attention de l'autre partie (le responsable du traitement par exemple) sur la sensibilité et l'importance des informations échangées (par exemple les « données personnelles »).

---

[658] En ce sens, V. not. J. Mestre (dir.), *Les principales clauses des contrats d'affaires*, Lextenso, 2011, V° *Clause de secret et de confidentialité* ; W. Dross, Clausier, 2e éd., Litec, 2011, V° Confidentialité.

[659] M. Jouen, *Négociations et obligations de confidentialité*, AJCA 2016, p.275.

L'obligation de confidentialité n'est donc pas une contrainte à respecter, il faut plutôt l'entendre comme un gage de sécurité pour l'une et l'autre des parties lorsque ces dernières négocient un contrat qui porte sur des informations sensibles.

L'obligation de confidentialité doit être considérée comme une protection relative aux « données personnelles ». C'est en quelque sorte une prise de conscience pour le responsable de traitement et pour le titulaire de la « donnée personnelle ». En effet, le premier intéressé ne pourra dégager sa responsabilité en cas de violation de la clause de confidentialité, tant le fait de rajouter une telle clause démontre le caractère non négligeable des « données personnelles », tandis que pour le second, l'insertion d'une telle clause a pour effet de garantir la sécurité autour des informations personnelles qu'il divulgue et donc par-là assurer un effet de quiétude pour ce dernier.

244. Si l'utilité des clauses de confidentialité n'est plus à démontrer, il convient à présent de s'intéresser à la validité de ces dernières. Le principal enjeu concernant la validité des accords de confidentialité résulte au moment de leur rédaction et repose, plus particulièrement, sur le contenu de ces derniers. « *Les parties doivent tout d'abord veiller à ce que le contenu de l'accord soit certain, c'est-à-dire que son objet soit précis et déterminé. La validité de l'accord de confidentialité suppose ensuite que son contenu soit licite* »[660].

Les parties doivent, en premier, lieu préciser l'objet sur lequel porte l'obligation de confidentialité en question, à savoir en l'espèce les données à caractère personnel.

A ce titre, il convient de respecter une première exigence à savoir que l'information, objet de l'obligation de confidentialité, ne doit pas être connue du public. A défaut, pour le dire autrement, l'engagement de confidentialité se trouverait privé de contenu[661].

---

[660] M. Jouen, *Négociations et obligations de confidentialité*, *Ibid*, p.275.

[661] Rappr. J. Mestre, préc : l'obligation de confidentialité serait ainsi privée « d'objet et de cause ».

En effet, quel intérêt d'insérer une clause de confidentialité portant sur une information publique, connu de tous ? Sur ce point, étant des informations *intuitu personae*[662], les « données personnelles » donnent pleine satisfaction à cette exigence. Une seconde contrainte est à noter, celle de déterminer avec précision et avec clarté les données et informations soumises à protection. Là encore, les « données personnelles », puisqu'elles émanent d'un individu en particulier sont, par nature, claires et précises.

Concernant la condition de licéité, la validité de l'accord de confidentialité suppose, enfin, que son contenu soit licite. Le respect à cet impératif ne semble guère poser problème lorsqu'il est confronté aux « données personnelles ». En effet, les informations personnelles d'une personne représentent le prolongement de celle-ci et à ce titre ont, par nature, un objet licite.

245. Si l'obligation de confidentialité est une assurance pour les personnes concernées permettant d'une part de sécuriser les données personnelles en interdisant toute divulgation de celles-ci, d'autre part ce mécanisme facilite l'intervention des responsables de traitements en attirant l'attention de ces derniers sur l'importance des données et les précautions à prendre pour les collecter et les utiliser.

Pour autant, l'obligation de confidentialité s'impose-t-elle d'elle-même, notamment aux salariés qui utiliseraient des informations sensibles dans le cadre d'une relation de travail ?

---

662 « *Expression lat. signifiant « en considération de la personne » employée pour caractériser les opérations dans lesquelles la personnalité de l'une des parties est tenu pour essentielle* », G. Cornu, *Vocabulaire juridique*, *Op.cit.*

B) L'obligation de confidentialité à l'égard de la donnée personnelle au cours du contrat de travail

246. Si durant une relation de travail, l'employeur est tenu de respecter les données personnelles de ses salariés, notamment pendant la phase de recrutement[663], au cours de l'exécution du contrat de travail[664], mais aussi lorsque celui-ci prend fin[665], qu'en est-il maintenant de l'obligation de confidentialité de salariés qui utilisent des données personnelles dans l'exercice de leur travail ?

Cette situation est l'occasion d'atténuer la portée de l'obligation de confidentialité sans toutefois l'éteindre complètement. En effet, si l'obligation de confidentialité fait partie intégrante du règlement européen[666], notamment pour la mise en œuvre du principe de sécurité du traitement, cette obligation ne semble pas toujours devoir, inéluctablement, s'imposer, ce qui ne veut pas dire, il faut le préciser, qu'elle doit être négligée.

247. Si le règlement européen prône une obligation de confidentialité globale, le cas précis d'un salarié qui utiliserait dans le cadre de ses fonctions des données personnelles, appartenant à l'entreprise ou à des personnes concernées, n'impose pas une telle obligation pour une raison simple que la jurisprudence a dégagé il y a déjà quelques années, par un arrêt du 19 octobre 1994[667], la chambre sociale de la Cour de cassation estimant qu'une employée « *qui était tenue par des fonctions qu'elle exerçait depuis plusieurs années au secret professionnel, n'avait aucune obligation de faire le serment de confidentialité que lui demandait l'employeur et qui présentait un caractère superfétatoire, vexatoire et désobligeant* ».

---

663 *V. supra §n°218.*

664 *V. supra §n°219.*

665 *V. supra §n°220.*

666 « *1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, 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, y compris entre autres, selon les besoins :b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement (...)* », RGPD art. 32 (1., b), *préc.*

667 Cass. soc., 19 octobre 1994, 93-40.653, Inédit.

Cette solution qui s'appliquait à l'époque au serment de confidentialité, semble aujourd'hui pouvoir se rapporter à l'obligation de confidentialité. En effet, si le règlement général sur la protection des données personnelles impose à l'employeur, en qualité de responsable de traitement, de prendre toutes les mesures adéquates pour garantir la sécurité des données personnelles qu'il collecte et qu'il utilise à des fins de traitement (celles de l'entreprise, celles de ses clients, mais encore celles de ses salariés), ni ledit règlement, pas même la loi, n'imposent, formellement, à l'employeur de faire signer à ses salariés une clause de confidentialité.

Si cette position est tout d'abord compréhensible, elle n'en est pas moins regrettable. D'un côté, il n'est pas anormal, dans certaines situations, de ne pas imposer à un salarié de se soumettre à une clause de confidentialité alors que celui-ci est déjà dépendant d'une obligation de loyauté prévue à l'article L. 1222-1[668] du Code du travail (faisant référence aux articles 1104[669] et 1194[670] du Code civil). D'un autre côté, lorsque le salarié manipule des données personnelles dites sensibles, une clause de confidentialité ou clause de non divulgation pourrait avoir du sens pour sensibiliser et rappeler à celui-ci qu'il doit avoir une attention renforcée dans l'exercice de sa mission.

248. Puisqu'actuellement, la priorité est à la protection des données personnelles, il aurait pu être opportun pour le règlement européen de protection des données d'intégrer plus clairement cette obligation de confidentialité afin d'attirer l'attention sur cet outil au service des données. Voilà pourquoi la Commission nationale de l'informatique et des libertés vient au soutien de cette carence en préconisant deux possibilités. Dans un premier temps, ladite commission conseille de prévoir une charte dédiée à cet effet dans le règlement intérieur de l'entreprise, en sachant que celle-ci est admise par le Conseil d'État

---

668 « *Le contrat de travail est exécuté de bonne foi* », C. trav., art. L. 1222-1.

669 « *Les contrats doivent être négociés, formés et exécutés de bonne foi. Cette disposition est d'ordre public* », C. civ., art. 1104 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

670 « *Les contrats obligent non seulement à ce qui y est exprimé, mais encore à toutes les suites que leur donnent l'équité, l'usage ou la loi* », C. civ., art. 1194 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

car il estime que son objet est « *d'informer les salariés que la communication desdits documents à des tiers serait constitutive d'une faute disciplinaire* »[671]. Dans un second temps, la Commission incite aux entreprises de faire signer un engagement de confidentialité (dont elle fournit un exemple) à chaque fois qu'un salarié est en position d'utilisateur de données, c'est-à-dire lorsque, dans le cadre de son activité, il traite des données personnelles[672].

L'arrêt de la Cour d'appel de Bordeaux du 20 février 2020[673] démontre que la question de l'obligation de confidentialité à l'égard de la donnée personnelle est, plus que jamais, une question d'actualité, elle qui a jugé que le licenciement d'un salarié pour faute grave était fondé puisque « *en transmettant ainsi au futur dirigeant d'une entreprise concurrente en création des données interne à son employeur en création des données internes à son employeur, M. R a violé son obligation de discrétion, de confidentialité et de loyauté* ».

249. Si dans un contrat il est possible de préciser les contours de l'utilisation des « données personnelles » et plus notamment, de protéger celles-ci en imposant qu'elles restent confidentielles, cette obligation ne semble pas pour autant assez protectrice et pour remédier à cela, les dispositions du Code pénal paraissent plus pertinentes.

C'est à ce titre qu'il faut, alors, s'intéresser au mécanisme de l'obligation de secret professionnel, lui qui permet au volet pénal, par la sanction, de s'impliquer pleinement dans la protection des données personnelles lesquelles pourront, de ce fait, valablement s'épanouir.

---

671 CE., 1 SS, 26 septembre 1990, n°108279, Inédit au recueil Lebon.

672 URL : https://www.cnil.fr/fr/securite-informatique-sensibiliser-les-utilisateurs

673 CA., Bordeaux, ch. soc. section A, 26 novembre 2020, n° 17/02270.

§2 Le caractère universel de l'obligation de secret à l'égard de la donnée personnelle

250. La meilleure façon de concevoir l'obligation de secret à l'égard de la donnée personnelle est de s'intéresser à l'une de ses représentations les plus caractéristiques à savoir celle du secret médical (B). Mais avant cela, il appartient de s'interroger sur la position de l'obligation de secret envers celle de confidentialité (A).

A) L'obligation de secret, une obligation de confidentialité améliorée

251. Si l'obligation de confidentialité signifie une interdiction pour le salarié de divulguer, à des tiers à l'entreprise ou bien même à ses collègues employés, des informations dont le caractère est confidentiel (puisque ces informations reposent sur l'entreprise, sur ses salariés ou encore sur sa clientèle)[674], l'obligation de secret semble similaire en ce qu'elle implique, également, de garder pour soi une information connue.

Toutefois, là où l'obligation de confidentialité est en rapport avec l'activité de l'entreprise, l'obligation de secret professionnel a trait, quant à elle, davantage, à la protection des secrets des personnes.

252. C'est surtout un autre point, plus notable, qui est utilisé pour différencier ces deux obligations, à savoir que si l'obligation de secret se démarque de l'obligation de confidentialité, c'est parce qu'elle peut être pénalement sanctionnée, ce qui renforce son caractère dissuasif.

Le secret professionnel est une règle déontologique dont la définition est prévue à l'article 226-13[675] du Code pénal, « *La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit*

---

[674] *V. supra §n°247.*

[675] C. pén., art. 226-13, *préc.*

en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende ».

La sévérité de la sanction prévue pour la violation du secret professionnel est tout à fait logique puisqu'elle est en rapport avec, d'une part l'obligation qu'il crée, d'autre part l'objet sur lequel celle-ci repose et enfin en lien avec les protagonistes.

Premièrement, l'obligation de secret professionnel impose une inaction, celle de garder pour soit une information intime qu'une personne a pris soin de dévoiler, il est donc justifié de sanctionner, aussi lourdement, celui qui contreviendrait à ce devoir. En ce sens, la jurisprudence a pris soin de préciser que l'obligation de garder le secret professionnel se manifeste par la volonté de « *garantir la sécurité des confidences qu'un particulier est dans la nécessité de faire à une personne dont l'état ou la profession, dans un intérêt général et d'ordre public, fait d'elle un confident nécessaire* »[676]. La Cour de cassation a, par ailleurs, cru bon de devoir ajouter qu'il fallait retenir une conception large de l'origine du secret, en ce qu'il peut être sciemment révélé mais aussi déduit ou, encore, même constaté « *Pour déclarer X coupable de violation de secret professionnel, les juges d'appel énoncent que le prévenu n'a pu avoir communication du dossier médical que « parce qu'il s'était présenté comme médecin » et que, des lors, il avait l'obligation de ne pas révéler, fut-ce à sa mandante « ce qu'il avait vu, entendu ou déduit en exerçant sa profession, même en l'absence de confidences du malade* »[677].

Ensuite, l'obligation de secret est d'une importance capitale du fait de l'information fournie. Ce mécanisme repose, en effet, sur une information intime, personnelle et propre à celui qui a cru bon devoir la confier. L'intérêt des informations divulguées étant majeur pour la personne concernée, il est cohérent de vouloir dissuader toute personne de rendre public de telles données personnelles par une peine d'emprisonnement.

Attention toutefois, si l'article cité condamne la pratique qui consiste à dévoiler un secret, la mise en œuvre de ce mécanisme est, seulement, pourvue à la

[676] Cass. crim., 19 novembre 1985, 83-92.813, Publié au bulletin.

[677] Cass. crim., 17 mai 1973, 72-91.572, Publié au bulletin.

condition que l'auteur des faits exerce une certaine profession, fonction, ou soit investi d'une mission précise. Sur ce point, la jurisprudence, précédemment évoquée, estime que toutes les révélations de confidences ne sont pas punissables, « *si celui qui a reçu la confidence d'un secret a toujours le devoir de le garder, la révélation de cette confidence ne le rend punissable que s'il s'agit d'une confidence liée à l'exercice de certaines professions* »[678].

A l'inverse, toujours pour s'assurer de l'entière préservation du secret des informations confiées, la jurisprudence s'est occupée de déterminer la portée et les contours de la révélation *strico sensu*, à savoir que pour qu'elle soit constituée, il suffit qu'une seule personne soit au courant, peu importe qu'elle soit elle-même tenue à une obligation similaire, « *La révélation d'une information à caractère secret est réprimée par l'art. 226-13 C. pén. n'en suppose pas la divulgation, et elle peut exister légalement, lors même qu'elle en est donnée à une personne unique et lors même que cette personne est elle-même tenue au secret* »[679].

Enfin, si la sanction de la violation de la présente obligation est si grave c'est parce qu'elle trahit une relation de confiance, relation que la que jurisprudence a, très tôt, caractérisé comme fondement du secret, « *En imposant à certaines personnes, sous une sanction pénale, l'obligation du secret comme un devoir de leur état, le législateur a entendu assurer la confiance qui s'impose dans l'exercice de certaines professions* »[680]. En effet, lorsqu'une personne choisit délibérément de communiquer des informations la concernant, elle le fait car elle a une entière confiance en son interlocuteur, par la fonction que ce dernier occupe (médecin, avocat, personnel de banque, etc.). Lorsque ce confident trahit le dépositaire d'information, il trahit en réalité sa fonction et donc sa déontologie.

253. L'obligation de secret professionnel est fortement liée à l'égard des données personnelles puisque cette obligation, au même titre que celle de confidentialité, repose sur des informations privées, que des personnes concernées ont souhaité confier à leurs interlocuteurs. Puisque bon nombre de professions

---

[678] *Ibid.*

[679] Cass. crim., 21 nov. 1874 : *S. 1875. 1. 89, rapp. Baudouin et note Cauwès.,* Cass. crim., 16 mai 2000 *:préc. note 8*.

[680] Cass. crim., 15 déc. 1885 *: DP 1886. 1. 347.*

bénéficient ou plutôt sont soumises à ce devoir, à savoir le respect au secret des informations qui ont été communiquées, la jurisprudence s'est, très rapidement, exercée, à donner une définition des personnes tenues au secret, « *L'art. 378 C. pén. s'applique à tous ceux auxquels leur état ou leur profession impose l'obligation du secret en ce qui concerne les faits dont la connaissance leur est parvenue en raison de l'exercice de leur profession* »[681].

Au fil des années, la jurisprudence s'est développée sur la question des personnes tenues au secret et de ce fait a pu répertorier, de manière non exhaustive, plusieurs exemples de professions soumis à ce devoir. Ainsi sont-ils tenus au secret professionnel, les avocats dont le secret professionnel « *couvre toutes les confidences qu'il a pu recevoir* »[682], les ministres de cultes (légalement reconnus) tels que les prêtres ou les curés qui doivent « *garder le secret sur les révélations qui ont pu leur être faites à raison de leurs fonctions* »[683], les banquiers dont l'obligation au secret « *ne cesse pas avec la résiliation du contrat conclu avec son client* »[684], ou encore les experts-comptables[685], les journalistes[686], les jurés[687], les notaires[688], les policiers[689] et bien sur les médecins[690] dont le secret médical sera détaillé par la suite.

254. Tant du point de vue de la loi que de la jurisprudence, l'obligation de secret est encadrée et le respect de celle-ci est assuré pleinement du fait de la peine d'emprisonnement instaurée en cas de violation de celui-ci. Si l'obligation de confidentialité et l'obligation de secret intéressent particulièrement les données personnelles, la seconde semble avoir un caractère hautement plus dissuasif.

---

681 Cass. crim., 17 juill. 1936 : *DH 1936. 494*.

682 Cass. civ. 1re, 7 juin 1983 : *Bull. civ. I, n° 169*.

683 Cass. crim., 4 déc. 1891 : *DP 1892. 1. 139*.

684 Cass. civ. 1re, 2 juin 1993, n° 91-10.971 P.

685 Cass. crim., 24 janv. 1957 : *Bull. crim. n° 86 ; D. 1957. 298. ; S. 1957. 219 ; Gaz. Pal. 1957. 1. 412*.

686 Cass. crim., 4 déc. 2007, n° 05-87.384 P : *AJ pénal 2008. 140, obs. Royer*.

687 Cass. crim., 25 janv. 1968 : *préc. note 7 ; rejet du pourvoi contre*.

688 Cass. crim., 7 avr. 1870 : *S. 1870. 1. 277*.

689 Cass. crim., 26 oct. 1995, n° 94-84.858 P.

690 Cass. crim., 8 mai 1947: *Bull. crim. n° 124 ; D. 1948. 109, note Gulphe ; JCP 1948. II. 4141, note Legal ; Gaz Pal. 1947. 2. 12*.

255. Il convient désormais de s'intéresser à une certaine forme du secret professionnel, dans un domaine particulier, dont la donnée personnelle est omniprésente, celle du secret médical.

B) L'étude approfondie de l'exemple type de l'obligation de secret à l'égard de la donnée personnelle : le secret médical

256. Bien qu'il soit présent dans la plupart des contrats (contrat de travail, contrat en lien avec la propriété intellectuelle et artistique), c'est particulièrement à l'égard de la donnée en matière de santé que le principe du secret professionnel permet de sanctionner de manière très claire la révélation des informations qui ont été confiées. Voilà pourquoi, naturellement, le règlement général sur la protection des données personnelles s'intéresse à cet enjeu.

Pour résumer l'attrait et l'intérêt du règlement européen de protection de données envers le secret médical, le vice-président du Conseil national de l'ordre des médecins, expert du numérique en santé, déclare que le règlement s'inspire du respect du secret professionnel et du secret médical, ce qui représente en réalité la traduction dans le monde numérique du secret hippocratique[691].

257. Si le secret médical est l'une des représentations les plus abouties et concrète de l'obligation de confidentialité qui existe à l'égard des données personnelles, en l'espèce des données de santé, c'est notamment parce que ce devoir est l'un des plus fondamentaux à respecter pour un professionnel de santé, un médecin par exemple. En effet, chaque médecin en début, mais aussi, tout au long de sa carrière professionnelle, est tenu de prêter, puis respecter, le serment hippocratique, lequel prévoit que « *Admis(e) dans l'intimité des personnes, je tairai les secrets qui me seront confiés. Reçu(e) à l'intérieur des maisons, je respecterais les secrets des foyers et ma conduite ne servira pas à corrompre les mœurs* »[692].

S'il n'a pas de valeur juridique, ce texte est l'un des fondateurs de la déontologie médicale. Il convient à ce propos de noter que la notion de secret y est présente à

---

691 Interview du Docteur J. Lucas par L. Martin, *Les obligations du médecin sur la protection des données personnelles (RGPD)*, M-soigner.com, URL : https://youtube.com/watch?v=sZ12bUTZXDw

692 URL : https://www.conseil-national.medecin.fr/medecin/devoirs-droits/serment-dhippocrate

deux reprises, ce qui en démontre l'importance au regard des informations et données qu'elle recouvre.

Ce texte n'est pas le seul garant du secret médical, puisque le Code pénal apporte, lui aussi, sa contribution en instaurant une sanction propre à la violation de ce principe.

Tout professionnel de santé est donc soumis à une obligation de maintien du secret, assortie de sanctions pénales. En effet, l'article 226-13 du Code pénal permet de sanctionner les atteintes au secret dans la mesure où l'obligation de conservation du secret constitue un impératif absolu pour le professionnel et, plus généralement, pour toute personne ayant connaissance d'une information à l'occasion de l'exercice de sa profession. L'article L. 1111-8 du Code de la santé publique vise, à cet égard, celui qui héberge et conserve la donnée de santé.

258. Il existe de très nombreuses dispositions destinées à garantir la personne contre les atteintes au secret professionnel concernant ses données de santé. Les articles L. 1110-4 du Code de la santé publique[693], et anciennement l'article L. 161-36-1 A. I du Code de la sécurité sociale[694], rappellent l'étendue du secret affirmant que « *toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant* ».

Le contrat conclu avec le professionnel inclut, en effet, une obligation de conservation du secret. Cette obligation consiste en une obligation de ne pas révéler d'informations protégées. Elle représente l'archétype de l'obligation de ne pas faire. La violation de ce type d'obligations engage la responsabilité du débiteur, sans preuve d'une faute. Il faut, et il suffit, pour bénéficier de l'indemnisation d'un dommage, que le résultat recherché – le maintien du secret – n'ait pas été obtenu.

---

693 CSP., art. L. 1110-4, *préc.*

694 C. sec. soc., art. L. 161-36-1 A.

259. Toutes ces dispositions, et d'autres relatives aux établissements par exemple, permettent une protection efficace du patient contre la violation du secret de ses données de santé à caractère personnel. De nombreux cas peuvent néanmoins se produire, dans lesquels aucune sanction ne pourrait éventuellement être prononcée. Il est possible d'évoquer, par exemple, la captation d'informations à caractère sanitaire par un pirate informatique qui n'est débiteur d'aucune obligation au secret. En cette hypothèse, les dispositions de l'article 226-13 du Code pénal s'avèrent inapplicables.

Il sera certainement préférable de saisir l'occasion de la publication des décrets relatifs au dossier médical personnel pour créer un régime complet de protection. Un tel régime présenterait l'avantage de ne laisser aucune situation hors de son champ d'application.

260. Le fait est certain, la donnée est d'abord et avant tout protégée par le secret professionnel. Étant de nature absolue, celui-ci s'impose, même au-delà du contrat.

C'est d'ailleurs ce que précise l'article 323-1 du Code pénal qui condamne l'accès et le maintien frauduleux en précisant que « *le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30.000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45.000 euros d'amende* »[695].

Si pour certains auteurs[696], le règlement général des protections met en œuvre certaines nouveautés, notamment en étendant la possibilité de procéder au traitement de certaines données sensibles sous couverture du secret professionnel à l'hypothèse de données dont la finalité est la lutte contre les menaces

[695] C. pén., art. 323-1.

[696] A. Deroudille, *Le secret professionnel dans le règlement général sur la protection des données (RGPD)*, RFDA n° 6, Novembre-Décembre 2018, p 1112, Dalloz 1er janvier 2019.

transfrontalières à la santé publique, le règlement européen démontre l'intérêt qu'il porte au secret professionnel et donc au respect des données personnelles de santé. Il suffit, pour s'en assurer, selon ces mêmes auteurs, de prendre en compte l'évolution du contenu dudit règlement européen, puisque si la référence à la notion de secret professionnel ne connaissait que trois occurrences dans la directive de 1995[697], cette notion apparait désormais une dizaine de fois dans le texte de 2016[698].

261. Si les deux manifestations que sont l'obligation de confidentialité et l'obligation du secret sont nécessaires à la protection des données personnelles, il convient à présent de s'intéresser au mécanisme de conservation des données, outil qui complète l'objectif principal du règlement général de protection des données personnelles.

[697] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, *préc.*, v. consid. (33), art. 8.3, et art. 28.7.

[698] RGPD consid. (53), (75), (85), (164), art. 9.2, i), 9.3, art. 14.5, d), art. 38.5, art. 54.2, art. 90.1, Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

Section 2 : Les obligations de protection et de conservation des données personnelles

262. Les obligations de protection des données personnelles doivent être rapprochées de la question de la conservation de celles-ci (Paragraphe 1) pour en étudier tous les problèmes qui y découlent (Paragraphe 2).

§1 Les obligations de protection quant à la conservation des données personnelles

263. Après avoir évoqué l'obligation de confidentialité à l'égard des données à caractère personnel, et notamment à l'égard des données de santé, il convient de s'intéresser à un autre mécanisme visant à protéger ces dernières.
En effet, cet autre mécanisme, dont le but est similaire à celui poursuivi par l'obligation de secret représente, en définitive, la finalité de celle-ci, à savoir la question de la conservation des données personnelles, également gage de protection de ces dernières.

A cet égard, Jean-Marc Mousseron expose ce mécanisme et allègue à ce sujet que « *L'obligation de secret consiste à ne pas relever certaines informations industrielles, commerciales ou autres, voire l'existence et le contenu de la négociation. Il s'agit, donc, d'une obligation de ne pas faire* »[699].

Le fait est donc certain, la donnée est d'abord et avant tout protégée par le secret professionnel, dont la traduction en pratique, c'est-à-dire sa mise en œuvre, passe nécessairement par l'enjeu de conservation. Étant de nature absolue, le secret professionnel s'impose pendant la durée même du contrat, mais également au-delà de celui-ci, voilà pourquoi la notion de conservation y est étroitement liée, puisqu'elle participe à sa bonne exécution.

[699] J-M. Mousseron, *Technique contractuelle,* Francis Lefebvre, 4e édition par P. Mousseron, J. Raynard, J.B. Seube.

Curieusement, l'exigence relative à la protection des données personnelles recouvre deux réalités, deux obligations, qui sont en apparence, seulement, contradictoires. En effet, pour s'assurer de l'exigence précitée, les responsables de traitement doivent, à l'encontre des personnes concernées et de leurs données personnelles, une obligation d'une part de confidentialité et de secret et d'autre part une obligation de conservation.

Derrière ces différentes problématiques apparaissent deux réalités pratiques, deux actions : l'une de faire quelque chose, l'autre à l'inverse de ne pas faire quelque chose. Pour respecter l'objectif de protection des données personnelles, le responsable de traitement devra, pour commencer, se soumettre à l'obligation de ne pas divulguer les informations qui lui sont parvenues et devra, ce qui est son corollaire, respecter l'obligation qui est celle de garder lesdites informations. Puisque la première obligation a été évoquée, il convient, cette fois, de se focaliser sur l'opération de conservation.

264. La question de l'obligation de protection relative à la conservation des « données personnelles » recouvre, en réalité, celle des entités qui ont pour fonction de conserver les données à caractère personnel des titulaires, ou de toute autre personne concernée.

Aussi, il convient de se demander quelles sont ces entités ? Un élément de réponse est apporté par le droit de la consommation qui précise que « *Toute personne physique ou morale qui assure, même à titre gratuit, pour la mise à la disposition du public en ligne, le stockage de signaux, d'écrits, d'images, sons et messages de toute nature, fournis par les destinataires de ces services, est un hébergeur* »[700]. Si la portée de la présente définition, reprise de loi pour la confiance dans l'économie numérique[701], est trop large, elle permet toutefois d'avoir un aperçu sur les hébergeurs et d'en comprendre la finalité.
C'est donc la jurisprudence de la Cour de cassation qui s'est efforcée de clarifier le statut de la notion d'hébergeur.

[700] Dictionnaire du vocabulaire juridique 2019, *Op cit.*

[701] Art. 6 I 2° de la loi n° 2004-575 du 21.06. 2004 pour la confiance dans l'économie numérique (LCEN).

Du fait de la définition, assez imprécise, de la notion d'hébergeur, il existait, en pratique, une difficulté avec une entité voisine, celle d'éditeur. En effet, la définition citée était source de conflit et de contentieux entre certains éditeurs qui avaient pour, mauvaise, habitude de se qualifier d'hébergeur[702]. Si certains éditeurs utilisaient un tel comportement, la raison était toute simple, la responsabilité des hébergeurs étant moindre, en se faisant passer pour de simple hébergeur leur responsabilité d'éditeur était bien amoindrie.

La disparité ou plutôt la nuance entre ces deux notions se trouve, bien évidement dans leur définition, mais elle concerne aussi et surtout leur mission. Chacune ayant une finalité bien précise, il est de ce fait logique que la responsabilité entre ces deux entités ne soit pas la même.
Si l'hébergeur est en quelque sorte un prestataire technique dont le but est d'assurer simplement la mise à disposition d'un serveur, voir d'une interface[703], de son côté l'éditeur est l'entité qui, par son rôle actif, est supposée avoir connaissance et avoir un pouvoir de contrôle sur l'ensemble du contenu diffusé sur son site internet[704].

Le degré d'implication de l'une et de l'autre entité à l'égard du contenu d'un site internet, c'est-à-dire à l'égard des données présentes sur ce site, dessine le degré de responsabilité de chacune. Plus l'entité est impliquée à l'égard des données personnelles, plus elle est responsable. A ce sujet, si l'éditeur est tenu de s'assurer de l'ensemble du contenu diffusé sur un site, tout en étant également soumis à une obligation de contrôle, l'hébergeur quant à lui bénéficie, à juste titre, d'un régime allégé de responsabilité, dans ce cas sa responsabilité ne peut être engagée que s'il

---

[702] URL : https://www.haas-avocats.com/actualite-juridique/justice-precise-statut-hebergeur-internet-procedure-suivre-engager-responsabilite/

[703] « *L'article 14 de la directive 2000/31 doit être interprété en ce sens que la règle y énoncée s'applique au prestataire d'un service de référencement sur Internet lorsque ce prestataire n'a pas joué un rôle actif de nature à lui confier une connaissance ou un contrôle des données stockées. S'il n'a pas joué un tel rôle, ledit prestataire ne peut être tenu responsable pour les données qu'il a stockées à la demande d'un annonceur à moins que, ayant pris connaissance du caractère illicite de ces données ou d'activités de cet annonceur, il n'ait pas promptement retiré ou rendu inaccessibles lesdites données* », CJUE, 23 mars 2010, *Google France et Google*, aff. C-236/08.

[704] URL : ttps://www.village-justice.com/articles/Hebergeur-editeur-hebergeur-editeur,16097.html

a été informé d'un contenu manifestement illicite et pour lequel il n'a pas agi promptement dans le but de le retirer.

265. L'enjeu entre ces deux entités étant déterminé, il est aisé de comprendre pourquoi certains éditeurs souhaitaient échapper à leur responsabilité en se faisant passer pour des hébergeurs, technique de manipulation que la jurisprudence de la Cour de cassation s'est permis de mettre en échec en établissant de manière stricte un statut propre à l'hébergeur.

En février 2011, la Cour de cassation a rendu deux décisions qui précisent et figent le statut de l'hébergeur. Dorénavant, doivent être qualifiés comme des hébergeurs les entités ou intermédiaires informatiques qui effectuent et réalisent des prestations purement techniques (arrêt dit « Dailymotion »[705]) dont l'objectif est notamment celui de faciliter l'usage du site internet par le public concerné (arrêt dit « Fuzz »[706]).

---

705 « *Mais attendu que l'arrêt relève que le réencodage de nature à assurer la compatibilité de la vidéo à l'interface de visualisation, de même que le formatage destiné à optimiser la capacité d'intégration du serveur en imposant une limite à la taille des fichiers postés, sont des opérations techniques qui participent de l'essence du prestataire d'hébergement et qui n'induisent en rien une sélection par ce dernier des contenus mis en ligne, que la mise en place de cadres de présentation et la mise à disposition d'outils de classification des contenus sont justifiés par la seule nécessité, encore en cohérence avec la fonction de prestataire technique, de rationaliser l'organisation du service et d'en faciliter l'accès à l'utilisateur sans pour autant lui commander un quelconque choix quant au contenu qu'il entend mettre en ligne ; qu'il ajoute que l'exploitation du site par la commercialisation d'espaces publicitaires n'induit pas une capacité d'action du service sur les contenus mis en ligne ; que de l'ensemble de ces éléments la cour d'appel a exactement déduit que la société Dailymotion était fondée à revendiquer le statut d'intermédiaire technique au sens de l'article 6-I-2 de la loi du 21 juin 2004* », Cass. civ. 1re, 17 février 2011, n° 09-67.896, n°165.

706 « *Mais attendu que la cour d'appel qui a relevé que l'activité de la société Bloobox net, créatrice du site www.fuzz.fr, se bornait à structurer et classifier les informations mises à la disposition du public pour faciliter l'usage de son service mais que cette société n'était pas l'auteur des titres et des liens hypertextes, ne déterminait ni ne vérifiait les contenus du site, en a exactement déduit que relevait du seul régime applicable aux hébergeurs, la responsabilité de ce prestataire, fût-il créateur de son site, qui ne jouait pas un rôle actif de connaissance ou de contrôle des données stockées ; qu'ainsi la cour d'appel qui n'était pas tenue de procéder à une recherche qui ne lui était pas demandée a légalement justifié sa décision* », Cass. civ. 1re, 17 février 2011, n° 09-13.202, n°164.

La Haute juridiction affine également sa position en effectuant un revirement de la jurisprudence dite « Tiscali »[707] puisqu'elle considère désormais que sera hébergeur celui qui accomplit des travaux et qui a une activité technique, sans se soucier de savoir si celui-ci exploite ou non, de manière lucrative, les contenus édités par certains internautes[708].

Depuis 2011, la jurisprudence considère que celui, à savoir une entité ou un prestataire, qui met en œuvre une activité d'hébergement en se cantonnant seulement à des opérations techniques sur les contenus présents sur les sites internet (à savoir du ré-encodage, de la classification par mots clefs, mais aussi du formatage etc.) en vue de leur diffusion aura nécessairement la qualité d'hébergeur.

Par ces différentes jurisprudences, la Cour de cassation met fin à l'insécurité juridique causée par l'ambiguïté existante entre les notions d'éditeur et d'hébergeur. Et par la même occasion, la jurisprudence affirme que la responsabilité de l'hébergeur ne pourra être engagée si ce dernier n'a eu qu'un rôle technique envers le contenu d'un site internet, à savoir notamment les données personnelles que celui-ci peut contenir. Cette position étant clarifiée, il ne sera plus possible pour un éditeur de se faire passer pour ce qu'il n'est pas, en l'occurrence un hébergeur, afin de voir sa responsabilité engagée. Désormais, la position étant claire, l'éditeur devra assumer ses responsabilités envers les données personnelles.

266. Afin de mieux caractériser ce que sont et surtout ce qu'apportent les hébergeurs de données en matière de conservation des « données personnelles »,

---

[707] « *Mais attendu que l'arrêt relève que la société Tiscali média a offert à l'internaute de créer ses pages personnelles à partir de son site et proposé aux annonceurs de mettre en place, directement sur ces pages, des espaces publicitaires payants dont elle assurait la gestion ; que par ces seules constatations souveraines faisant ressortir que les services fournis excédaient les simples fonctions techniques de stockage, visées par l'article 43-8 de la loi du 30 septembre 1986 dans sa rédaction issue de la loi du 1er août 2000 applicable aux faits dénoncés, de sorte que ladite société ne pouvait invoquer le bénéfice de ce texte, la décision de la cour d'appel est légalement justifiée ; que le premier moyen n'est donc pas fondé et le second est inopérant* », Cass. civ. 1re, 14 janvier 2010, n° 06-18.855, Publié au bulletin.

[708] Cass. civ. 1re, 17 février 2011, n° 09-67.896, n°165, *préc*.

il convient de s'intéresser à ces entités lorsqu'elles sont au service du domaine de la santé.

En effet, le domaine de la santé regroupe bon nombre d'informations capitales au sujet des patients, et à ce titre, il est essentiel que les « données personnelles » de ces derniers se retrouvent sous l'ombre d'entité capable d'en assurer la protection.

Une fois encore, il est possible de donner un exemple intéressant à l'égard des tiers qui sont supposés conserver les données sanitaires. Issus de la loi du 13 août 2004 qui est à l'origine du dossier médical personnel, ces hébergeurs de données de santé se sont vus dotés d'un cadre réglementaire assez strict, cadre que le règlement général sur la protection des données personnelles a fait évoluer.

Il convient pour se faire de s'intéresser à l'article L. 1111-8 du Code de la santé publique puisqu'il permet de mettre en lien les hébergeurs de données et les données à caractère personnel en précisant que ces entités devront, logiquement, être en conformité avec le règlement général sur la protection des données. En effet, la prestation d'hébergement réalisée par les hébergeurs de données s'apparente à un traitement de celles-ci et cela ne peut se faire qu'en respectant le règlement européen.

267. Plus que de seulement montrer le lien qui existe entre les hébergeurs de données et les données de santé, cet article est également intéressant parce qu'il démontre que le règlement européen a influencé son contenu, toujours dans un souci de protection. Voilà pourquoi si lors de sa création par la loi du 4 mars 2002[709], l'article L. 1111-8[710] du Code de la santé publique traitait de l'agrément

[709] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé (1).

[710] « *Les professionnels de santé ou les établissements de santé ou la personne concernée peuvent déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, auprès de personnes physiques ou morales agréées à cet effet (…). Les conditions d'agrément des hébergeurs sont fixées par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés et des conseils de l'ordre des professions de santé ainsi que du conseil des professions paramédicales. Ce décret mentionne les informations qui doivent être fournies à l'appui de la demande d'agrément, notamment les modèles de contrats prévus au deuxième alinéa et les dispositions prises pour garantir la sécurité des données traitées en application de l'article 29 de la loi n° 78-17 du 6 janvier 1978 précitée, en particulier les mécanismes de contrôle et de sécurité dans le*

des hébergeurs de données de santé, aujourd'hui avec l'article L. 1111-8[711] du même Code de la santé publique modifié par l'ordonnance du 12 janvier 2017[712] il est question de cas de certification des hébergeurs de données de santé.

La pratique d'agrément, qui reposait autrefois sur la bonne foi du prestataire hébergeur, ne faisait pratiquement l'objet d'aucun contrôle. Ce manque de sérieux envers les données de santé, pourtant qualifiées de sensibles, a conduit à rehausser le degré de protection envers ces entités qui conserve lesdites données. Désormais, le respect des exigences souhaitées directement par le Ministère de la Santé, examiné au travers de la Délégation à la stratégie des systèmes d'information de santé et de l'Agence du numérique en santé, sera contrôlé et audité par un organisme externe, aux frais de l'hébergeur[713], lors d'une procédure dite de certification.

Selon l'Agence du numérique en santé[714], la procédure de certification repose sur une évaluation de conformité au référentiel de certification. L'hébergeur de santé doit choisir un organisme certificateur qui devra lui-même pour avoir cette qualité être accrédité par le Comité français d'accréditation (ou par un équivalent au niveau européen).

L'organisme procède ensuite à un audit en deux étapes afin d'évaluer la conformité de l'hébergeur de données aux exigences du référentiel de certification. L'organisme cité vérifie notamment l'équivalence des éventuelles

domaine informatique ainsi que les procédures de contrôle interne », CSP., art. L. 1111-8 (Création Loi n°2002-303 du 4 mars 2002 – art. 11() JORF 5 mars 2002).

711 « *II. L'hébergeur de données mentionnées au premier alinéa du I sur support numérique est titulaire d'un certificat de conformité. S'il conserve des données dans le cadre d'un service d'archivage électronique, il est soumis aux dispositions du III. Ce certificat est délivré par des organismes de certification accrédités par l'instance française d'accréditation ou l'instance nationale d'accréditation d'un autre État membre de l'Union européenne mentionnée à l'article 137 de la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie. Les conditions de délivrance de ce certificat sont fixées par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés et des conseils nationaux de l'ordre des professions de santé* », CSP., art. L. 1111-8, *préc.*

712 Ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel.

713 URL: https://www.mysih.fr/hds-de-lagrement-a-la-certification/

714 URL : https://esante.gouv.fr/labels-certifications/hds/certification-des-hebergeurs-de-donnees-de-sante

certifications « ISO 27001 ou ISO 20000 » déjà obtenues par l'hébergeur. Il faut savoir que la première étape est relative à l'audit documentaire, c'est-à-dire que l'organisme certificateur réalise une revue documentaire du système d'information du candidat hébergeur afin de déterminer la conformité documentaire du système par rapport aux exigences du référentiel de certification. Ensuite, la seconde étape est relative à l'audit sur site, en ce sens, les preuves d'audit sont recueillies dans les conditions définies dans le référentiel d'accréditation.

Lorsque ces deux étapes sont réalisées, l'hébergeur dispose de trois mois après la fin de l'audit sur site pour corriger les éventuelles non-conformités et faire auditer ses corrections. Lorsque ce délai de trois mois est passé et sans aucune action de l'hébergeur, toute la procédure d'audit sur site sera de nouveau réalisée.

Lorsque toutes les étapes sont terminées, le certificat est enfin délivré pour une durée de trois ans, par l'organisme certificateur et chaque année, un audit dit de surveillance est effectué.
C'est une réalité, l'exigence de protection relative aux hébergeurs à l'égard des données personnelles s'est considérablement renforcée ces dernières années. La nouvelle procédure de certification des hébergeurs est bien plus conséquente que celle concernant l'agrément de ces derniers.

Les certificateurs qui valident et qui contrôlent la bonne exécution des hébergeurs à l'égard des données de santé étant des entités extérieures, la qualité du suivi est irréprochable.

Il faut se réjouir d'une telle avancée, la question de la protection et par la celle de la conservation des données de santé, données dites sensibles, est un enjeu primordial. Les hébergeurs de santé qui ont la lourde responsabilité de conserver lesdites données ont désormais la confiance des personnes concernées.

268. Si l'obligation de protection, à travers celle de conservation des données, est une nécessité pour un souci de sécurité, il est possible toutefois de rencontrer quelques difficultés à ce sujet, surtout concernant la logique de responsabilité.

§2 Le problème lié aux obligations de protection des données personnelles

269. La protection des « données personnelles » est nécessairement un problème lié à la responsabilité des responsables de traitement et plus particulièrement avec le rapport qu'ils entretiennent avec les sous-traitants dont ils font appel. Si les questions relatives aux responsables de traitements ont déjà été évoquées, il convient de s'attarder sur la question de la protection des « données personnelles » lorsqu'elles sont traitées par des sous-traitants. Ainsi, il est intéressant de s'interroger sur la responsabilité des sous-traitants au prisme du Règlement général de protection des données personnelles ?

270. En droit français, la sous-traitance est définie par l'article 1er de la Loi du 31 décembre 1975 comme « *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 maitre de l'ouvrage* »[715].

Cette définition permet de rendre compte qu'en matière de sous-traitance, l'entrepreneur est le responsable. C'est exactement le même constat qui est donné par la Cour de cassation lorsqu'elle énonce que « *La faute du sous-traitant engage la responsabilité de l'entrepreneur principal à l'égard du maitre de l'ouvrage* »[716].

271. S'il est possible d'affirmer que la responsabilité du sous-traitant est, en droit français, protégée, qu'en est-il sous l'autorité du règlement général de protection des données ?

Au regard du Règlement UE 2016/679, le sous-traitant représente « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui*

---

[715] Art. 1er, Loi n° 75-1334 du 31 décembre 1975, *préc.*

[716] Cass. civ. 3eme, 11 mai 2006, n° 04-20.426 P : *RDC 2006. 1214, obs. Viney*.

traite des données à caractère personnel pour le compte du responsable du traitement »[717].

Il ne faut donc pas confondre ces deux notions. Responsable de traitement et sous-traitant étant différents, le second étant en effet au service du premier. A cet égard, l'article 28 *in fine* du règlement européen précise que si un organisme détermine la finalité et les moyens de traitement, il ne peut en aucun cas être qualifié de sous-traitant, mais plutôt comme le véritable responsable de traitement[718]. Le sous-traitant est en réalité celui qui traite des « données personnelles » à la demande et pour le compte d'un responsable de traitement.

Avant l'entrée en vigueur du règlement général sur la protection des données, seul le responsable de traitement était finalement responsable en tant que décideur principal des finalités et moyens du traitement dont il était question.

Tout ceci a vocation à changer avec l'entrée en matière de ce dernier. En effet, l'attachement du règlement au principe de « responsabilisation des acteurs de traitement », déjà évoqué, à vocation à s'imposer à toute entité qui traite des « données personnelles », le cas de la sous-traitance ne semble pas y échapper.

272. Dans cet esprit, le règlement général sur la protection des données impose aux sous-traitants toute une série d'obligations à respecter.

Premièrement, dans l'exercice de leur mission les sous-traitants doivent mettre en œuvre « *des garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées de manière ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée* »[719]. Les sous-traitants ont donc obligation, pour le bien

---

[717] RGPD art. 4, *préc.*

[718] « *Sans préjudice des articles 82, 83 et 84, si, en violation du présent règlement, un sous-traitant détermine les finalités et les moyens du traitement, il est considéré comme un responsable du traitement pour ce qui concerne ce traitement* », RGPD art. 28 *in fine, préc.*

[719] RGPD art. 28 *in limine*, *préc.*

de leur client, d'être en conformité totale avec le Règlement général sur la protection des données.

Ensuite, le sous-traitant à une autre obligation à respecter qui est celle de ne traiter les « données personnelles » que sur instruction du responsable de traitement. Si cette obligation n'était pas respectée, le sous-traitant outrepasserait ses pouvoirs et prendrait le risque de se voir requalifié en tant que responsable du traitement. Sous l'ère du règlement européen, les sous-traitants ont donc peu de marge de manœuvre, mais cela est dans leur intérêt.

Dans l'hypothèse où le sous-traitant a désigné un délégué à la protection des données, dont la mission est de piloter la conformité du au règlement européen au sein de l'organisme qui l'a désigné, le premier doit coopérer avec le second. En effet, l'article 38 du présent règlement relatif à la « Fonction du délégué à la protection des données » estime que « *Le responsable du traitement et le sous-traitant aident le délégué à la protection des données à exercer les missions visées à l'article 39 en fournissant les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées* »[720].

Pour mener à bien leurs missions, les sous-traitants ont aussi obligation, au même titre les responsables du traitement, de coopérer avec la Commission nationale de l'informatique et libertés afin de démontrer le bien fondée de celles-ci. Le considérant 82 du règlement européen prévoit à ce titre que « *Chaque responsable du traitement et sous-traitant devrait être tenu de coopérer avec l'autorité de contrôle* »[721].

273. Les cas de figure relatifs aux obligations des sous-traitants étant terminées, il convient de s'intéresser plus particulièrement sur le principe de l'engagement de la responsabilité des sous-traitants tel que perçu par le règlement européen.

[720] RGPD art. 38, *préc.*

[721] RGPD consid. 82, *préc.*

A l'égard de la responsabilité des sous-traitants, le règlement général sur la protection des données semble innover et impose une fracture avec la responsabilité contractuelle des sous-traitants au prisme du droit français. En effet, le problème de la protection des « données personnelles » n'est plus réservé aux seuls responsables du traitement. Le respect qui incombe au souci de protection des « données personnelles » est aujourd'hui, aussi, celui des sous-traitants, qui deviennent dès lors responsables.

L'article 82, alinéa 4, du règlement européen affirme en ce sens que, « *Lorsque plusieurs responsables du traitement ou sous-traitants ou lorsque, à la fois, un responsable du traitement et un sous-traitant participent au même traitement et, lorsque, au titre des paragraphes 2 et 3, ils sont responsables d'un dommage causé par le traitement, chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective* »[722].

Cet article démontre toute la logique et le renouveau inscrit par ledit règlement, toujours dans le souci de protection des « données personnelles ». La logique réparatrice mise en avant par le règlement oblige désormais les sous-traitants, au même titre que les responsables de traitements de tout mettre en œuvre pour assurer l'entière protection des « données personnelles », et ce pour éviter toute sanction.

Pour en terminer avec l'étude des sous-traitants et leur respect au règlement européen dans le bien fondé des « données personnelles », il faut ajouter que les sanctions administrées aux sous-traitants seront les mêmes que pour les responsables défaillants. La conformité au dit règlement doit donc être un moteur tant pour les responsables du traitement que pour les sous-traitants, au risque de se voir lourdement sanctionné[723].

[722] RGPD art. 82 al. 4, *préc.*

[723] RGPD art. 82, *préc.*

274. Comme il a déjà été démontré[724], la situation peut se poser également en matière sanitaire puisque sans réellement se référer à la notion de sous-traitance, la loi impose aux professionnels, services et organismes de santé, dépositaires de données personnelles et sanitaires de les faire héberger auprès de tiers, anciennement agréés, dorénavant certifiés.

Le cadre de cet hébergement de données est strictement encadré par la loi qui précise que toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, doit se soumettre aux conditions que l'article L. 1111-8[725] du Code de la Santé publique précise.

Non seulement les hébergeurs de données de santé ne peuvent pas utiliser les données qui leur sont confiées à d'autres fins que l'exécution de la prestation d'hébergement, mais encore sont-ils soumis à des règles de respect du secret et de l'obligation de confidentialité avec autant de rigueur que n'importe quel autre tiers. Ils sont en cela contrôlés par les autorités de l'État, et peuvent être sanctionnés, tant au plan civil que pénal.

A ce sujet, un arrêt récent de la Cour d'appel de Paris peut être pris en exemple pour démontrer les obligations qui incombent, mais également celles qui n'incombent pas aux hébergeurs de donnée de santé.

En effet, bien plus que de simples formalités, les obligations dont les hébergeurs de données de santé sont soumis font office de référence en cas de mise en cause, en cas de responsabilité de ces entités. Comme cela a été le cas concernant les missions de ces prestataires, à propos des missions purement techniques de ces derniers, la jurisprudence, toujours dans un souci de sécurité, de protection, s'est

---

[724] *V. supra §n°265.*

[725] CSP., art. L. 1111-8, *préc.*

intéressée à préciser les cas dans lesquels la responsabilité des hébergeurs ne devait pas être recherchée.

Ainsi, selon un arrêt de la 8e chambre rendu en date du 1er mars 2019[726], l'hébergeur de donnée n'étant pas responsable du traitement des données à caractère personnel, il ne lui incombe pas d'effectuer une quelconque démarche relative à l'exploitation des sites internet, ou à celle des services de mise en relation, type de formalités prévues par la Commission nationale de l'informatique et des libertés, éventuel recueil du consentement, informations relatives aux activités de commerce électronique via ces sites internet. La Cour d'appel justifie sa position par le fait qu'il n'existait pas de trouble manifestement illicite à rechercher sur ce fondement.

Si dans cet exemple, la jurisprudence expose un cas où il n'est pas nécessaire de rechercher la responsabilité des hébergeurs, d'autres arrêts sont rendus cette fois contre les hébergeurs.

L'intérêt et l'apport du travail réalisé par la jurisprudence est de préciser et d'encadrer la situation de ces entités afin de s'assurer du respect qui est dévolu aux données de santé et plus généralement aux données personnelles. Si cette entreprise est celle de la jurisprudence, bien évidemment, tant la loi mais aussi et surtout le règlement européen contribuent à ce souci de protection des données, ainsi, chacun œuvre pour renforcer la sécurité des personnes concernées et par là celle des données personnelles.

---

[726] « *Par ailleurs, il n'est justifié, ni prétendu, d'aucune notification du contenu illicite relative au site. Ainsi c'est à bon droit que le premier juge a retenu que la société OVEXA ayant la qualité d'hébergeur de contenus, M. C-D ne justifiait pas de la notification préalable en cas de contenus illicites prévue par la loi du 21 juin 2001 et que sa responsabilité civile ne pouvait être engagée. Il s'ensuit que la preuve n'est pas établie qu'au jour où le premier juge a statué il existait un trouble manifestement illicite, la condition préalable de mise en œuvre de la responsabilité civile de la société X hébergeur n'est pas remplie. Par ailleurs, n'étant pas responsable du traitement des données à caractère personnel, il ne lui incombe pas d'effectuer une quelconque démarche relative à l'exploitation des dits sites internet, ou à celle des services de mise en relation, type formalités CNIL, éventuel recueil du consentement, informations relatives aux activités de commerce électronique via les dits sites internet, de sorte que nul trouble manifestement illicite ne peut être recherché de ces chefs. La décision de première instance sera confirmée de ce chef* », CA., Paris, pole 1, ch. 8, 1er mars 2019, n°18/15084.

275. L'obligation de protection des données personnelles comporte des exigences de confidentialité et de secret pour les personnes qui usent et qui traitent des données, dont la finalité est le mécanisme de conservation de celles-ci par certaines entités notamment des hébergeurs certifiés lorsque les données personnelles sont les plus sensibles, tel que c'est le cas concernant les données de santé.

276. Si la problématique de l'exécution d'un contrat portant sur les données personnelles amène à s'intéresser aux enjeux de l'utilisation et de la protection de celle-ci, il convient se demander ce qu'il se passe en cas d'inexécution des obligations pourtant sur les données personnelles ?

CONCLUSION DU CHAPITRE 2

Notion particulièrement sensible, l'utilisation de la donnée personnelle est soumise à certaines obligations, ce qui est notamment le cas de l'obligation de confidentialité et de l'obligation de secret.

Puisque la donnée personnelle mérite une attention particulière, les obligations citées sont, pour ce faire, corroborées par une obligation de protection, mais également de conservation, à l'égard de celle-ci.

CONCLUSION DU TITRE 1

277. L'exécution des contrats portant sur les données personnelles se caractérise par la conception de deux types d'obligations propres à ces dernières. En effet, si certaines obligations sont en lien direct avec l'utilisation de la donnée personnelle, d'autres sont en revanche au service de la protection de celle-ci.

278. Différents cadres législatifs ou réglementaires permettent la détermination de l'utilisation des données personnelles permettant ainsi de savoir ce qu'il est possible de faire ou de ne pas faire, lorsque les contrats reposent sur les données personnelles.

En sus, plusieurs obligations s'attachent à la protection des données, c'est le cas notamment pour les obligations de confidentialité ou celles de protection et de conservation des données personnelles.

TITRE 2

L'inexécution des obligations portant sur les données personnelles

279. La question qui se pose alors est de savoir comment se trouverait sanctionné le fait de divulguer, d'utiliser ou de récupérer à des fins illicites les données en lien avec un contrat.

280. C'est d'abord et avant tout au regard du contrat qu'il conviendra de s'interroger sur le devenir de celui-ci (Chapitre 1), avant de s'interroger sur les autres sanctions applicables (Chapitre 2).

Chapitre 1 : Les sanctions au regard du contrat

281. Si le contrat est le mécanisme juridique qui paraît être exposé en cas de violation de la donnée personnelle (Section 2), c'est d'abord et avant tout la défaillance de celui qui viole la donnée dans le contrat qui l'expose également à un plan plus personnel (Section 1).

Section 1 : Les sanctions liées à la responsabilité du contractant défaillant

282. Le contractant défaillant peut-être, tout à tour, l'utilisateur des données personnelles ou aussi bien le titulaire de celles-ci. Les sanctions liées à la responsabilité du contractant défaillant touchent donc tant le premier (Paragraphe 1) que le second (Paragraphe 2).

§1 Les sanctions qui frapperaient le contractant qui utilise les données personnelles

283. Si la question des sanctions relatives au contractant défaillant qui utilise des données personnelles est traitée au sein de cette seconde partie, il ne faut, pourtant, pas en déduire que cette problématique est secondaire, bien au contraire. La question de la responsabilité est au cœur de la réglementation général sur la protection des données, règlement qui opère une révolution en imposant aux responsables de traitement une obligation de pouvoir démontrer qu'ils se conforment à son égard[727].

Si une telle démarche relève en droit français du principe de responsabilité, en matière de données personnelles son équivalent a pour synonyme le terme d'« *accountability* » dont la traduction est celle de l'idée de « rendre compte de ». En ayant recours au principe d'*accountability,* le présent règlement s'appuie et utilise un état d'esprit pour la sauvegarde des données personnelles, à savoir le fait de se responsabiliser. Avec ce système d'autocontrôle, chaque responsable de traitement doit donc être en mesure de prouver que le traitement des données personnelles qu'il réalise est conforme aux attentes du règlement général de protection des données. L'avantage de ce mécanisme, en plus d'insuffler la crainte d'une sanction, est qu'il fait supporter aux responsables de traitement l'enjeu de leur propre responsabilité. En effet, il revient à ces derniers de tout mettre en

[727] K. Rosier et A. Delforge, *Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD*, Éditions Larcier, 16/11/2018, p. 665 et s.

œuvre pour, d'une part, se conformer audit règlement et, d'autre part, de démontrer cette démarche. En définitive, la question de la responsabilisation des acteurs, qui utilisent les données personnelles, intéresse la question des sanctions car elle comporte un intérêt pour les autorités de contrôle. Ces derniers disposent de plus de facilité pour contrôler le bon usage des données personnelles (puisqu'il suffit de vérifier le travail préparatoire de conformité déjà réalisé par les responsables de traitement), ce qui implique une meilleure efficacité pour sanctionner les responsables de traitement potentiellement désobéissant.

Voilà pourquoi, pour asseoir son autorité et pour renforcer son but premier, celui de s'assurer de la protection des données personnelles, le règlement général sur la protection des données personnelles porte une attention toute particulière au régime de sanctions pour violation de sa propre réglementation, attention qui émane du souhait du législateur européen d'améliorer l'effectivité des règles relatives au traitement de données[728].

284. Traiter des sanctions qui frapperaient le contractant qui utilise les données personnelles, c'est naturellement s'intéresser aux difficultés causés par un responsable de traitement, lui qui collecte et utilise les données, sans pour autant négliger la présence d'un autre acteur également au centre de la question de la protection des données en cas de traitement inadéquat, à savoir le sous-traitant.

En effet, si l'entrée en application du règlement européen n'est pas une révolution en soit, le régime de responsabilité à l'égard des données personnelles étant déjà présent dans la directive de 1995[729], elle qui prévoyait à l'article 23[730] que « *Les États membres prévoient que toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la présente directive a le droit d'obtenir du responsable du traitement réparation du préjudice subi* », cette obligation était cantonnée au seul responsable de traitement. Désormais, en cas d'inexécution ou d'exécution

[728] L. Gérard, *Les sanctions en cas de non-respect du RGPD : vers une plus grande effectivité de la protection des données à caractère personnel* ?, Éditions Larcier, 16/11/2018, p. 641 et s.

[729] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, *préc.*

[730] Art. 23, Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, *préc.*

malveillante, relative au traitement de données personnelles, le contractant qui utilise celles-ci pourra être soit le responsable de traitement, soit un sous-traitant lorsque celui-ci joue un rôle dans ledit traitement de données[731].

285. Si la question des sanctions est aussi importante c'est parce qu'elle vient finaliser la logique de responsabilité, maintes fois mise en avant par le règlement général sur la protection des données. C'est bien l'idée d'une sanction qui impose et justifie le mécanisme de responsabilité. Contraindre les responsables de traitement à se responsabiliser, sans crainte de sanction n'aurait aucun sens. Lorsque celui qui contourne le règlement de protection des données, qui s'affranchit des règles en vigueur, cause du tort aux données personnelles, mais aussi et surtout aux personnes concernées, il doit assumer et réparer.

Voilà pourquoi, il convient de s'intéresser aux sanctions que pourrait rencontrer le contractant défaillant qui utilise les données c'est-à-dire d'une part le responsable de traitement (A) et d'autre part, ce qui est un apport du règlement UE 2016/679, le cas du sous-traitant, également responsable en cas de traitement de données non satisfaisant (B).

A) Le responsable de traitement, premier contractant défaillant en ce qui concerne les données personnelles

286. Comme le définit l'essence même de l'article 1101 déjà cité, le contrat n'est rien d'autre qu'un accord de volonté[732]. De ce fait, si les parties ne sont plus d'accord, si l'une ou l'autre des parties néglige son engagement ou outrepasse son obligation, alors le contrat n'est plus.

Aussi, tout contractant qui ne remplirait pas ses obligations, engage sa responsabilité. En effet, tout contractant défaillant est responsable et doit en assumer les conséquences. Tel est le principe même de la responsabilité

---

[731] K. Rosier et A. Delforge, *Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD*, *Op cit*, p. 665 et s.

[732] C. civ., art. 1101, *préc.*

contractuelle qui se décrit comme « *l'obligation pour un contractant qui n'exécute pas les obligations nées de son contrat de réparer le dommage subi par son cocontractant* »[733]. Pour résumer, la responsabilité contractuelle est donc une sanction pour le contactant qui commet une faute en ne respectant pas ses engagements.

Toute la difficulté peut porter sur la détermination de ce que l'on entend par « faute » dans l'inexécution ou dans la mauvaise exécution du contrat, et plus encore de s'interroger sur le fait de savoir si un comportement « illicite » en lien avec le contrat peut caractériser l'idée d'une « faute » au sens commun susceptible d'engager la responsabilité du contractant.

287. Aussi, convient-il, par un exemple, de concrétiser l'étude de la responsabilité contractuelle en en tant que sanction du cocontractant qui utilise les « données personnelles ». Voici le cas suivant dans lequel l'enseigne de commerce de détail d'appareils électroménagers « DARTY » (entendu en tant que responsable de traitement) vend un pèse-personne connecté à un particulier (au sens de titulaire de « données personnelles »).

En l'espèce, pour que le contrat ait valablement lieu, il faut que « DARTY » livre le pèse-personne en question et que le particulier divulgue des informations personnelles le concernant tel que son poids, sa taille, son âge, ses antécédents médicaux afin de faire fonctionner l'appareil, informations qui sont en réalité des « données personnelles » propre à chacun.

Pour ce faire, le titulaire de données (le particulier) accepte de divulguer des « données personnelles » le concernant et donne son accord à « DARTY » pour que l'enseigne transfère ces informations au fournisseur, lequel mettra tout en œuvre pour que le pèse-personne connecté fonctionne en adéquation avec son propriétaire.

[733] Dictionnaire du vocabulaire juridique 2019, *Op cit.*

Si jamais « DARTY » décide, en plus de transférer les informations personnelles du particulier au fournisseur, de vendre ces « données personnelles » à une société de boissons telle que « PEPSICO », qu'elle en est l'incidence ?

Par cette attitude, c'est-à-dire par la vente commerciale de « données personnelles », l'enseigne « DARTY » commet une faute, vis-à-vis du contrat en violant l'obligation de confidentialité protégeant les « données personnelles » et vis-à-vis du droit commun en violant le règlement général sur la protection des données et le droit pénal (notamment l'article 226-13 du Code pénal).

288. Dans le souhait de démontrer ce à quoi correspond la violation d'une obligation en rapport avec les « données personnelles », il parait, tout d'abord, judicieux de s'intéresser à la notion de secret professionnel.

Le secret professionnel est entendu comme « *l'obligation, dont le respect est sanctionné par la loi pénale, imposant à certains professionnels de taire les informations, à caractère secret, dont ils sont dépositaires, soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire. L'incrimination implique la révélation, par le professionnel, de confidences qui lui ont été faites ou d'éléments recueillis au cours de l'exercice de son activité, portant ainsi atteinte à la confiance nécessaire à l'exercice de certaines professions ou fonctions* »[734].

289. Lorsque ledit secret professionnel est évoqué, il faut, en réalité, s'intéresser également à l'obligation de non-divulgation d'informations confidentielles. Au sens des « données personnelles », le responsable de traitement à donc, de par sa qualité, de par sa fonction, interdiction de divulguer à qui que ce soit les informations personnelles que la personne concernée lui aurait dévoilées. Ainsi par exemple, pourrait-on considérer que la violation du secret, au-delà de son volet pénal, constitue au plan civil une véritable violation d'une « obligation contractuelle de confidentialité » dont la sanction pèsera sur le contractant défaillant. L'enseigne « DARTY » serait donc coupable d'une faute et devrait, au

[734] Lexique des termes juridiques, *préc.*

titre de la responsabilité civile contractuelle, allocation de dommage intérêts envers le particulier.

Après le volet civil, c'est ensuite le cadre du Règlement général sur la protection des données qui se prête particulièrement à cette situation, spécifiquement quant à l'assimilation de la violation du secret à la violation d'une obligation de confidentialité. En effet, selon l'article 90 du règlement général sur la protection des données, « *Les États membres peuvent adopter des règles spécifiques (…), à l'égard des responsables du traitement ou des sous-traitants qui sont soumis (…), à une obligation de secret professionnel ou à d'autres obligations de secret équivalentes »*[735].

Le règlement européen laisse donc le soin, aux États membres, en l'occurrence au droit français, de régir les atteintes au secret professionnel, ce qui est fait à travers les dispositions de l'article 226-13 du Code pénal qui prévoit que « *La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15.000 euros d'amende* »[736].

290. Le droit pénal vient donc au secours du droit des contrats et par la même occasion au secours des « données personnelles » en protégeant la non-divulgation afférente à ces informations intimes et en offrant la possibilité de voir dans la violation générale de la confidentialité des données issues d'un contrat un élément permettant de caractériser la faute civile. La question était déjà évoquée bien avant que n'entre en vigueur le règlement européen de 2016[737], elle se pose avec encore plus de rigueur aujourd'hui.

Au plan purement pénal, et de surcroît, le fait d'émettre la possibilité d'une peine de prison et d'une amende pécuniaire pour toute personne qui violerait le secret

[735] RGPD art. 90, *préc.*

[736] C. pén., art. 226-13, *préc.*

[737] V. C. Féral-Schuhl, *Cyberdroit*, *Le droit à l'épreuve de l'internet*, Dalloz, 8e Edition, 2020.

professionnel permet de renforcer la protection des informations divulguées par la personne concernée. Aussi, par ces dispositions, au même titre qu'un avocat, un banquier, un médecin ou un assureur, un responsable de traitement, est soumis au secret professionnel concernant les « données personnelles » que son cocontractant lui a dévoilé.

S'il est possible que des informations intimes, secrètes, soient dévoilées, sous conditions, comme le précise l'article 226-14 du Code pénal[738], la règle reste la protection des « données personnelles » découlant de la relation de confiance inséré dans le contrat entre la personne concernée et le responsable de traitement. De ce fait, en cas de divulgation d'informations personnelles, sans l'accord du titulaire des « données personnelles », le responsable de traitement est responsable puisque défaillant au titre d'une violation de son obligation de protection envers ces dernières.

291. Si l'article 1104 du Code civil impose un principe de bonne foi contractuelle[739], il arrive que l'un ou l'autre des cocontractants soit défaillant et donc à ce titre responsable.

Lorsqu'il s'agit d'évoquer la responsabilité et les sanctions qui frapperaient le contractant qui utilise les données personnelles, celle du responsable de traitement est la principale cible. Cet acteur, qui était jusque-là le seul responsable de la protection des données, mais aussi, de toutes les conséquences que cela pouvait engendrer, est désormais, depuis l'entrée en application du règlement européen de protection des données, l'équivalent sur le plan des responsabilités d'un autre acteur qui collecte, utilise, traite également des données personnelles à savoir le sous-traitant.

---

[738] C. pén., art. 226-14 (*L. n° 2004-1 du 2 janvier 2004, art. 11*).

[739] *« Les contrats doivent être négociés, formés et exécutés de bonne foi »,* C. civ., art. 1104, *préc.*

B) Le sous-traitant, nouveau contractant responsable en cas d'inexécution à l'égard des données personnelles

292. Il faut savoir que toutes les règles évoquées en amont, à savoir celles qui précisent et sanctionnent la responsabilité des responsables de traitement défaillant, s'appliquent et se transposent à l'encontre des sous-traitants, acteurs ayant, à propos des données personnelles, un rôle secondaire mais, non moins, actif, eux qui étaient jusque-là protégés.

En effet, avant l'entrée en vigueur du règlement général sur la protection des données, le système de responsabilité prévu était simple puisqu'il reposait entièrement et uniquement sur le responsable de traitement, le sous-traitant devait présenter des garanties suffisantes[740] pour assurer la mise en œuvre des mesures de sécurité et de confidentialité, exigence qui ne déchargeait pas le responsable du traitement de son obligation de veiller au respect de ces mesures[741].

Le rôle du sous-traitant était donc limité, il avait pour objectif de mettre en œuvre des mesures pour assurer et garantir la protection des données personnelles, mais ce, sans réelle obligation ni contrainte. Pour le dire simplement, si le sous-traitant connaissait des failles dans sa mission, il ne risquait rien, toute la logique de responsabilité était en réalité supportée par une seule entité, à savoir le responsable de traitement.

Pour les données personnelles, un tel mécanisme n'était pas bénéfique, bien au contraire, la sur-responsabilisation du responsable du traitement de celles-ci faisait émerger un paradoxe, celui d'affaiblir la protection des personnes physiques sur leurs données personnelles[742]. Il n'était pas judicieux de faire reposer une telle responsabilité, à l'égard d'informations aussi intimes et sensibles, sur une seule entité, les responsables de traitement, ces derniers n'ayant,

---

[740] Art. 34, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (*Version en vigueur du 07 aout 2004 au 01 juin 2019)*.

[741] RGPD, *Guide du sous-traitant*, Edition septembre 2017, p. 5.

[742] URL : www.village-justice.com/articles/rgpd-responsabilite-sous-traitant-peut-plus-etre-evitee,38225.html

en pratique, pas la capacité technique, ni les connaissances suffisantes afin de réaliser cette démarche. L'accroissement, toujours, exponentiel d'utilisation, de partage, de transmission, de collecte de données personnelles à l'échelle internationale a rendu nécessaire le fait de modifier le régime de responsabilité à l'égard des données pour s'adapter aux échanges de données sur le marché.

293. Avec l'entrée en vigueur du règlement UE 2016/679, le sous-traitant n'est plus comme par le passé, relégué au second plan, son rôle actif envers les données personnelles est accentué ce qui entraine, fort logiquement, un renforcement de ses responsabilités. Le sous-traitant est au même titre que le responsable du traitement un acteur majeur, il n'est plus un simple exécutant, voilà pourquoi il devient à son tour responsable de ses actions réalisées à l'encontre d'un traitement de données personnelles.

C'est, notamment, à travers deux articles que le présent règlement détaille le nouveau rôle qui incombe au sous-traitant, rôle dont la logique de protection et de responsabilité est naturellement renforcée ce qui va de pair avec une implication dans le traitement de donnée renforcée. Si l'article 28[743] du règlement relatif à la protection des données personnelles énonce que « *Lorsqu'un traitement doit être effectué pour le compte d'un responsable de traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée* », l'article 32[744] vient quant à lui signaler que « *(...) le responsable de traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ».

A lecture de ces deux articles, il apparait que la responsabilité du sous-traitant au traitement de données personnelles est clairement affichée, ce dernier ne peut plus se « cacher » derrière le responsable de traitement. Le règlement européen

[743] RGPD art. 28, *préc.*

[744] RGPD art. 32, *préc.*

instaure un principe de collaboration, de répartition entre ces deux acteurs, responsables de traitement et sous-traitant, dans lequel chacun réalise une mission sans toutefois couper le lien qui existe entre eux, ce qui impact nécessairement la question de la responsabilité qui ne reposera plus uniquement sur le seul responsable de traitement, mais qui sera également partagée avec le sous-traitant.

En instaurant ce procédé, l'objectif du règlement général de la protection des données est, toujours en accord avec ses convictions, celui de défendre aux mieux les intérêts des personnes concernées et de leurs données personnelles. Voilà pourquoi les articles cités expriment l'idée d'une répartition des tâches et des responsabilités, dans un esprit collaboratif, obligeant pour chaque acteur intervenant sur le même traitement de données de collaborer pour garantir aux personnes concernées une meilleure protection de leurs données[745].

294. Pour démontrer l'effectivité des nouvelles règles énoncées par le présent règlement, il parait intéressant de s'intéresser à une décision rendue le 27 janvier 2021[746] par la Commission nationale de l'informatique et des libertés, décision qui résume, au surplus, la question de la responsabilité ainsi que celles d'éventuelles sanctions en cas de contractant défaillant, en l'occurrence celle d'un sous-traitant, suite à une mauvaise exécution de traitement de données personnelles.

Par cette décision, si la Commission nationale de l'informatique et des libertés rappelle que de manière classique, traditionnelle, il appartenait au responsable de traitement de décider des mesures de sécurité adéquates à mettre en place afin d'assurer la protection du traitement, celui-ci ne pouvait pas, pour ce faire, simplement déléguer à un sous-traitant la mission de remédier aux difficultés survenues suites à certaines attaques par *credential stuffing*[747] portées contre son

---

745 URL : www.village-justice.com/articles/rgpd-responsabilite-sous-traitant-peut-plus-etre-evitee,38225.html

746 Délibération de la formation restreinte n° SAN-2021-003 du 12 janvier 2021 concernant le ministère de l'intérieur.

747 URL : https://www.cnil.fr/fr/la-violation-du-trimestre-attaque-par-credential-stuffing-sur-un-site-web

site internet[748]. De plus, si le responsable de traitement, en l'espèce, a été tenu pour responsable de ne pas avoir utilisé les techniques sécuritaires de traitement les plus adaptées, la présente Commission innove et retient par ailleurs la responsabilité du sous-traitant qui aurait dû, lui aussi, au même titre que le responsable du traitement, rechercher toutes les solutions favorables afin d'assurer la protection des données personnelles en les proposant au responsable de traitement. Puisque cela n'a pas été réalisé, une violation de l'obligation d'accompagnement et de conseil du sous-traitant a été caractérisée, voilà pourquoi la décision, retenant la faute de ces deux acteurs, prononce et inflige une sanction au *prorata* de la responsabilité de chacun.

Par cette décision, la Commission nationale de l'informatique et des libertés démontre l'apport du règlement, lui dont l'objectif est celui de tout mettre en œuvre pour s'assurer de la protection des données personnelles. En admettant la possibilité d'administrer des sanctions pour les sous-traitants défaillants, les données personnelles voient leur protection augmentée. Le responsable de traitement ne supporte plus le poids de sa défaillance, désormais s'il peut être considéré comme fautif, un sous-traitant peut l'être également. Aussi, lorsqu'une de ces deux entités réalise un traitement de données léger, l'autre peut lui rappeler ces obligations et par là servir les intérêts des personnes concernées et de leurs données personnelles.

295. En s'intéressant aux sanctions possibles au regard du contrat, notamment aux sanctions liées à la responsabilité du contractant défaillant, en l'espèce celui qui utilise les données personnelles, c'est-à-dire l'entité qui collecte et traite celles-ci, il est possible de comprendre les avancées du présent règlement.

Il est vrai que le règlement général sur la protection des données personnelles protège la personne concernée par les « données personnelles » contre les responsables de traitement, mais également contre les sous-traitants qui peuvent jouer un rôle dans ledit traitement, pour autant, il arrive que le cocontractant

[748] URL : https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant

défaillant ne soit pas, toujours, celui à qui penser en premier. Il est possible, dans de rares situations, que le titulaire de « données personnelles » soit, lui-même, à l'origine de défaillance.

§2 Les sanctions qui frapperaient le titulaire de la donnée personnelle

296. Si comme cela vient d'être démontré, l'utilisateur de la « donnée personnelle » peut engager sa responsabilité pour non-respect de son obligation en ce qui concerne la protection des « données personnelles » qui lui sont confiées et violer l'obligation de garantir le secret de ces informations, quel serait le risque si la violation ou la simple négligence dans l'utilisation des « données personnelles », tout à l'inverse, émanait, cette fois, du titulaire de la « donnée personnelle » ?

L'hypothèse évoquée ici est la suivante, bien que le titulaire de la « donnée personnelle » soit le plus souvent victime, le voilà placé en situation d'auteur du dommage ou de générateur du dommage. Est-il possible de lui opposer le fait de la victime pour minimiser son dommage ? Si la question se pose en droit civil commun, elle pourrait ne pas forcément s'appliquer au droit particulier des données, c'est pourquoi il faudra s'interroger sur le fait de savoir si le règlement général sur la protection des données prévoit cette hypothèse.

297. Avant d'évoquer la question au prisme du Règlement général sur la protection des données, il convient de se pencher sur le droit général, et de se demander si le titulaire de la « donnée personnelle », lui-même, peut à son tour, engager sa responsabilité ?

Comme l'évoque l'article 1104, précité ci-dessus, « *Les contrats doivent être négociés, formés et exécutés de bonne foi* »[749]. Ce principe de « bonne foi contractuelle » s'adresse naturellement aux deux parties qui négocient, forment et exécutent un contrat.

De ce fait, appliquer à l'espèce, la bonne foi intéresse tant le responsable de traitement qui utilise la « donnée personnelle » que le titulaire entendu au sens de « personne concernée » par l'utilisation de ses « données personnelles ». Aussi, le mécanisme de réciprocité oblige donc les deux parties d'un contrat à maintenir,

[749] C. civ., art. 1104, *préc.*

poursuivre et respecter leur engagement, et cela à l'aune d'une bonne foi contractuelle évidente.

En effet, en présence d'un contrat passé entre un responsable de traitement et un titulaire de « donnée personnelle », si le premier s'engage à utiliser et protéger les « données personnelles » conformément à la volonté du titulaire de « données personnelles »[750], le second, c'est-à-dire la personne concernée par le traitement, s'engage quant à lui à délivrer une ou plusieurs informations conformes la concernant.

En conséquence, si jamais un titulaire de « donnée personnelle » s'engage envers un responsable de traitement en lui délivrant, sciemment, des informations qui ne sont en rien conforme avec la réalité, il devient un cocontractant défaillant et ne respecte donc pas ses obligations contractuelles.

298. Pour mieux saisir les propos développés précédemment, voici l'exemple d'une situation entre un équipementier sportif (en qualité de responsable de traitement) et un particulier (en tant que titulaire de « donnée personnelle »).

Un équipementier sportif propose à un particulier de répondre à un sondage afin de faire évoluer sa gamme de produits. En échange des informations personnelles délivrées par le particulier, l'équipementier sportif lui offre une séance de sport gratuite. Si le particulier répond au sondage en donnant de fausses informations le concernant, l'enquête réalisée par l'équipementier sportif sera erronée, en conséquence ce dernier ne pourra pas faire évoluer sa gamme de produits correctement.

Le titulaire de « donnée personnelle » devient donc auteur du dommage puisqu'en délivrant de mauvaises informations le concernant, il se rend coupable d'une mauvaise exécution contractuelle, ce qui crée un dommage pour l'autre partie. A ce titre, le titulaire de la donnée peut voir sa responsabilité civile contractuelle engagée. Dans une autre hypothèse, si jamais le responsable de traitement utilise

[750] C. civ., art. 1101, *préc.*

les fausses informations personnelles à des fins malveillantes, la victime pourrait voir son dommage minimiser puisqu'il commet tout de même une faute en donnant délibérément des informations erronées le concernant, donc en violant à son tour le respect de l'obligation de bonne foi contractuelle.

299. Cette pratique qui consiste à délivrer de fausses informations dans le but de brouiller les pistes est malheureusement courante de nos jours. En effet, la méfiance des titulaires de donnée envers la collecte et plus encore l'utilisation qui ait faite de leurs « données personnelles » pousse la population française à agir en ce sens.

Pour preuve, une étude réalisée en 2018 par l'observatoire des comportements de consommation révèle que 59 % des français avouent donner de fausses informations à ceux qui collectent leurs « données personnelles ». L'étude dresse un constat simple en indiquant que « *Peu confiants, les français ont développé des parades anti-collecte de données* »[751].

300. Du point de vue moral, un titulaire de « données personnelles » qui délivre, sciemment, de fausses informations le concernant, ne peut pas rester impuni. En effet, comment justifier le fait d'imposer au responsable de traitement une mise en conformité, sans faille, avec le règlement général sur la protection des données, sous peine d'amende pécuniaire et de peine de prison en cas de non-respect de celui-ci, et de l'autre laisser les personnes concernées par l'utilisation de leurs « données personnelles » induire en erreur les responsables de traitement ?

A ce titre, il est donc regrettable que le règlement ne sanctionne pas les titulaires de « données personnelles » qui délivreraient, en toute connaissance de cause, de fausses informations les concernant. Il semble que le règlement général sur les protections des données ait mis l'accent sur la protection des titulaires de « données personnelles », sans se soucier des actions négatives que ces derniers pourraient avoir.

---

[751] Observatoire des comportements de consommation, *La collecte de données personnelles sur les sites de e-commerce*, étude complète de Mai 2018, Odoxa – Emakina.

Il ne faut pas perdre de vue que pour tout contrat, l'une et l'autre des parties doit tirer profit sur ce pour quoi elle s'engage, sinon elle ne le ferait pas. Dans un contrat, aucune partie ne peut minimiser ou outrepasser ses engagements, pour le dire autrement, nulle partie ne peut être supérieure à l'autre.

301. Si le règlement général de protection des données personnelles semble ne s'intéresser au titulaire de « donnée personnelle » que lorsqu'il est en position de victime de l'utilisation de ses informations, sans s'intéresser à la situation dans laquelle il pourrait être auteur d'un dommage, le droit commun, quant à lui, ne laisse pas la situation sans réponse, puisque sur le principe général de la « bonne foi », il sanctionne toutes les hypothèses ou le titulaire de la donnée est générateur d'un dommage, notamment lorsqu'il délivre des informations erronées le concernant.

Heureusement, le droit commun permet de faire respecter l'équilibre contractuel existant entre les parties et vient sanctionner celle des parties qui aurait une intention malveillante envers son cocontractant.

Dans l'esprit de l'exemple susvisé, deux délits peuvent retenir une attention particulière dans le but de comprendre pourquoi certaines sanctions sont prises à l'encontre d'un titulaire de données personnelles.

Alors que les personnes concernées semblent plutôt être des cibles contre les responsables de traitement qui profiteraient de la faiblesse de ces derniers, il arrive qu'ils soient aussi acteurs de certaines malveillances à l'égard des données personnelles. Il est donc logique que ces actes désobligeants soient réprimandés, l'idée derrière cela est le fait de légitimer et justifier la protection accordée à ces personnes. En sanctionnant les personnes concernées lorsqu'elles agissent, ainsi, dans de mauvaises intentions, il est équitable par la suite de protéger ces dernières lorsqu'elles sont attaquées.

302. Pour entrer dans le vif du sujet, il convient, dès lors, de s'intéresser à la notion d'usurpation d'identité et à celle de faux intellectuel.

Si le plus souvent ce sont les responsables de traitement qui collectent et usent des données personnelles à l'insu des personnes concernées pour en tirer profit, il arrive que certaines personnes agissent malhonnêtement en usurpant l'identité d'autres personnes afin d'en obtenir des avantages.

Les moyens techniques et technologiques font que de plus en plus la technique d'usurpation d'identité se répand sur internet. Il est très simple pour une personne de s'accaparer des noms et prénoms d'une personne, du pseudonyme qu'elle utilise sur internet, de son adresse électronique, ou encore, de sa photographie. En résumé, il est très facile pour une personne de copier, voler, en définitive, d'usurper le profil numérique d'une personne.

Lorsqu'une personne réussit à accaparer l'identité numérique d'une autre personne, il lui est alors possible de faire différentes actions, telles que souscrire un abonnement ou un crédit au nom de la personne, ou situation plus banale mais tout aussi critique, il lui est possible de nuire à la réputation de celle-ci en envoyant des messages, en laissant des commentaires désobligeants ou en publiant des annonces farfelues.

Puisque l'utilisation d'internet est sans cesse en développement, il a été question, pour le bien des personnes concernées, de leur identité et donc de leurs données personnelles, de pénaliser le délit d'usurpation d'identité numérique par la loi d'orientation et de programmation pour la performance de la sécurité intérieure du 2 mars 2011[752], loi permettant la création de l'article 226-4-1 du Code pénal ainsi rédigé, « *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, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne* »[753].

[752] Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

[753] C. pén., art. 226-4-1.

L'intérêt de cet article et qu'il vise, au-delà de la simple usurpation d'identité commise de manière générale, plus largement l'usage « d'une ou plusieurs données de toute nature », ce qui permettra ainsi d'inclure dans la répression qu'il met en œuvre toutes nouvelles atteintes liées aux technologies telle que l'usurpation au mot de passe, au pseudonyme, à l'adresse mail, voire à l'adresse IP, qui ne représentent pas en tant que tels des usurpations d'identité, au sens classique, mais qui peuvent conduire aux mêmes dommages pour la victime[754].

Lorsqu'une personne est concernée par un tel agissement, il lui est conseillée premièrement de s'assurer que le profil en question qui semble utiliser, ses informations privées, ses données personnelles, n'est pas celui d'un homonyme[755]. Lorsque cette vérification est réalisée et que le trouble existe réellement, alors il convient, ensuite, de collecter un maximum d'éléments pour prouver l'infraction, il peut s'agir de captures d'écrans, de justificatifs ou même de l'adresse web des pages internet concernées. S'il possible de contacter directement l'auteur de l'infraction pour faire cesser le trouble et pour lui demander la suppression des informations concernant la personne usurpée, c'est-à-dire la victime, il est également possible, et c'est le but de l'article cité, de déposer une plainte pénale auprès d'un commissariat de police, d'une gendarmerie ou du procureur de la République[756].

La sanction prononcée à l'article 226-4-1 du Code pénal est une des manifestations des sanctions qui frappent le titulaire de la donnée personnelle lorsque celui-ci agit avec de mauvaises intentions. Si l'usurpation d'identité numérique est une des formes courantes des agissements trompeurs sur internet, le mécanisme du faux intellectuel représente fidèlement, quant à lui, un cas dans lequel le titulaire de la donnée personnelle, lui-même, trompe son cocontractant.

303. Le faux intellectuel résume l'exemple énoncé par lequel une personne concernée délivre sciemment de fausses informations à son sujet ce qui tronque

754 F. Mattatia, *RGPD et droit des données personnelles*, *Op cit*, p. 154.

755 URL : https://www.cnil.fr/fr/comment-reagir-face-une-usurpation -didentite

756 URL: https://www.pre-plainte-en-ligne.gouv.fr

la relation qu'il entretient avec un responsable de traitement qui collecte ses données personnelles. Si cet usage peut être motivé par la crainte des personnes concernées face aux géants d'internet, responsables de traitement, il n'en reste pas moins que cette pratique est interdite et sanctionnée. En effet, dans la situation précédente, il existe un échange de bon procédé entre l'équipementier sportif, en qualité de responsable de traitement, et la personne concernée sollicitée. Ainsi, si le particulier dévoile des informations tronquées à son sujet, il bénéficiera quand même de l'avantage prévu à cet effet, à savoir, en l'espèce, une séance de sport gratuite alors qu'il se rend coupable d'une inexécution contractuelle. Par cette manœuvre, la responsabilité de la personne pourra être engagée, le responsable de traitement ayant quant à lui exécuté convenablement le contrat en offrant ladite séance de sport prévue.

Aussi, afin de dissuader tout titulaire de données personnelles qui serait malintentionné, bien plus que d'engager seulement la responsabilité de ce dernier lorsqu'il partage de mauvaises informations à son sujet, ce qui a pour conséquence de tronquer la confiance du responsable de traitement, le volet pénal intervient à son tour pour sanctionner lourdement une telle inaction par l'article 441-1 du Code pénal[757] qui désigne le faux comme première atteinte à la confiance, « *Constitue un faux toute altération frauduleuse de la vérité, de nature à cause un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques. Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45 000 € d'amende* ».

En matière de données personnelles et pour reprendre l'exemple précédent, il semble que la personne titulaire de données personnelles se rende coupable, lorsqu'elle délivre des informations erronées à son sujet, d'un faux intellectuel, inaction qui représente la dissimulation intentionnelle d'informations ou l'affirmation de fausses informations. A ce sujet, bon nombre de jurisprudences permettent d'évoquer en pratique les cas d'usurpations d'identité sur internet,

[757] C. pén., art. 441-1.

ainsi une personne a été jugée pour avoir créé, par vengeance, sur un réseau social un faux profil d'un de ses anciens associés pour délivrer des messages diffamatoires et insultants[758], une autre avait été jugée pour avoir piraté le site web d'une personnalité publique[759], une jeune femme avait, également, été jugée, pour s'être vengée de son ex-amant en nuisant à sa réputation par la création de faux profil[760] ou encore a été jugé celui qui a créé un site internet calomnieux avec le nom et prénom d'une personne avec laquelle elle était en conflit[761].

304. Si le plus souvent ce sont les responsables de traitement qui agissent avec malhonnêteté, leur but étant de capter le plus d'informations sensibles et privées sur des personnes afin de pouvoir les revendre et donc en tirer profit, il arrive que les titulaires de données personnelles se placent, non plus en victime, mais bien en acteur capable de tromper et tronquer la relation de confiance qui est censée exister avec le responsable de traitement.

A ce sujet, si le règlement général sur la protection des données s'attache, fort logiquement, à sécuriser et protéger les personnes concernées et donc également leurs propres données personnelles, il est toutefois regrettable de ne pas trouver au sein de ce dit règlement de mentions relatives au comportement à adopter pour les personnes concernées.

Tous les plus grands principes du règlement européen, principe de licéité, loyauté et transparence, principe de finalité du traitement, principe de minimisation, principe de limitation de la conservation des données, respect et sécurité des personnes concernées etc., semblent directement intéresser les responsables de traitement, mais ne semblent pas s'imposer aux personnes concernées.

305. Le règlement général sur la protection des données personnelles est un atout majeur et permet un apport considérable pour les personnes concernées et la

---

[758] CA., Paris, 10 octobre 2014 : CCE janv. 2015, com. 9, note E.-A. Caprioli, Légipresse. 2015.51.

[759] TGI., Paris, 10 octobre 2014, confirmé CA Paris, 13 novembre 2015 et Cass. crim., 16 novembre 2016, n° 16-80.207, NP, CCE 2017, comm. 6, obs. A. Lepage ; Dr. pén. 2010, comm. 2, note P. Conte ; RLDI 2017/33, n° 4428.

[760] TGI., Paris, 17e ch. corr., 24 mars 2015, V. P. et F. Z. c/A. S et K. G., CCE 2015, comm. 86, obs. E.-A. Caprioli et CA Paris, 13 avril 2016.

[761] CA., Paris, Pôle 1, ch. 08, 19 janvier 2018, n° 16/24282, NP, Inédit, JurisData, Contentieux judiciaire.

sécurité de leurs données personnelles, pour autant, s'il impose de nombreuses obligations à l'encontre des responsables de traitement, il aurait pu également s'intéresser à avertir les personnes concernées sur les comportements à adopter. La notion d'exemplarité des personnes concernées aurait pu être abordée et mise en avant pour légitimer en retour le souci de sécurité qui est consacré à ces dernières. Malheureusement, malgré les efforts du règlement européen à l'égard des données personnelles, certaines personnes abusent de leur position. Si le plus souvent, il s'agit des responsables de traitement ou sous-traitant, il arrive, dans des cas plus rares, que certains actes malhonnêtes soient à attribuer aux personnes concernées.

306. Il ne faut pas oublier que le traitement de données personnelles est un contrat entre un responsable de traitement et une personne concernée, il faut donc établir une confiance entre les deux parties et pour ce faire, chacune doit respecter ses engagements, au risque de voir certaines sanctions frapper le contrat.

Section 2 : Les sanctions frappant le contrat

307. Lorsqu'une partie est engagée par un contrat et qu'elle n'exécute pas ses obligations, elle doit pouvoir être sanctionnée. C'est la traduction factuelle de la force obligatoire du contrat qui prévoit à ce titre que, « *Les contrats légalement formés tiennent lieu de loi à ceux qui les ont faits* »[762]. A cet effet, l'article 1217 nouveau du Code civil énumère cinq sanctions pouvant être mises en œuvre par le créancier d'une obligation lorsque celle-ci est inexécutée.

Il dispose ainsi, dans sa rédaction issue de la loi de ratification qui est venue en clarifier le sens, que : « *La partie envers laquelle l'engagement n'a pas été exécutée ou l'a été imparfaitement, peut : refuser d'exécuter ou suspendre l'exécution de sa propre obligation ; poursuivre l'exécution forée en nature de l'obligation ; obtenir une réduction du prix ; provoquer la résolution du contrat ; demander réparation des conséquences de l'inexécution* »[763].

308. Confrontées à la notion de « données personnelles », si certaines sanctions du contrat, au-delà du contractant, paraissent envisageables (Paragraphe 1), une autre est pour le moins probable (Paragraphe 2).

§1 Les sanctions envisageables

309. La mise en œuvre des sanctions relève du choix du créancier étant entendu qu'elles peuvent se cumuler lorsqu'elles ne sont pas incompatibles et que des dommages et intérêts peuvent toujours s'y ajouter (art. 1217 al. 2 nouveau du Code civil)[764]. Les anciennes dispositions du Code civil n'envisageaient que trois sanctions, à savoir, l'exécution forcée, la résolution judiciaire et les dommages et intérêts.

---

[762] C. civ., art. 1103, *préc.*

[763] C. civ., art. 1217 al. 1er *(Ord. nº 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

[764] C. civ., art. 1217 al. 2 *(Ord. nº 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

Seules l'annulation du contrat, la réduction du prix et l'exception d'inexécution seront ici étudiées en tant que sanctions envisageables lorsque l'inexécution du contrat porte sur des « données personnelles ».

310. L'annulation du contrat est une sanction frappant les conditions de formation du contrat, autrement dit, la nullité est la sanction judiciaire en cas de manquement à l'une des conditions de validité du contrat qui entraine l'anéantissement rétroactif de celui-ci. L'article 1178 nouveau du Code civil précise, en ce sens, que « *Un contrat qui ne remplit pas les conditions requises pour sa validité est nul* »[765]. L'emploi du terme « nul » signifie que le contrat est censé n'avoir jamais existé et c'est au juge qu'il revient de prononcer cette sanction bien qu'il soit, désormais, possible pour les parties de la constater d'un commun accord[766]. Pour autant, cette nouveauté ne semble, toutefois, pas envisageable tant il parait douteux que les parties s'entendent et conviennent, ensemble, de la nullité d'un contrat. Si pour certains auteurs l'innovation de l'article présentée, c'est-à-dire cette nullité « amiable »[767], risque d'être inutile, d'autres regrettent, à leur tour, que le législateur n'ai pas intégré dans ce texte le mécanisme de la conversion par réduction, lequel est utilisé avec parcimonie par la jurisprudence afin de sauver, de revaloriser, certains actes juridiques[768].

Toujours à propos de l'annulation du contrat, l'article 1179 du Code civil consacre la *summa divisio* des nullités en expliquant que « *La nullité est absolue lorsque la règle violée a pour objet la sauvegarde de l'intérêt général. Elle est relative lorsque la règle violée a pour seul objet la sauvegarde d'un intérêt privé* »[769]. En introduisant cet article dans le Code civil, à l'occasion de la réforme du droit des obligations, le législateur a souhaité mettre fin au débat, relatif aux critères de

---

765 C. civ., art. 1178, *préc.*

766 Y-M. Serinet, *La constatation de la nullité par les parties : une entorse limitée au caractère judiciaire de la nullité*, JCP 2016, p 845. (P. Lipinski, *La conversion des actes juridiques*, RRJ 2002/3, p. 1 – A. Boujeka, *La conversion par réduction, contribution à l'étude des nullités des actes juridiques formels*, RTD com. 2002. 223).

767 C. Gijsbers, *L'incidence des règles relatives à la nullité, à la caducité et aux restitutions*, RDI 2016, p. 342.

768 N. Dissaux, *Contrat : formation – Détermination des conditions, Op. cit.*

769 C. civ., art. 1179 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

distinction entre nullité absolue et nullité relative en délaissant la théorie dite classique et en consacrant « *ce qu'il est convenu d'appeler la théorie moderne des nullités* »[770].

Si la nullité relative est celle qui intéresse le contrat portant sur les « données personnelles » en tant qu'informations intimes du titulaire, l'annulation ne semble pour autant pas être une sanction pertinente lorsque l'inexécution du contrat est en lien avec les « données personnelles ». En effet, l'annulation suppose une atteinte relative aux conditions de formation du contrat. Si un responsable de traitement dévoile des informations personnelles sans l'accord de la personne concernée, ce n'est donc pas une condition de validité du contrat qui pose problème. Aussi, annuler un contrat en lien avec les données personnelles, lorsque la sanction repose sur l'utilisation de celle-ci, ne doit pas se faire sur ce fondement-là.

311. Si l'annulation du contrat ne semble pas une sanction pertinente, qu'en est-il de l'hypothèse de la réduction du prix ?

La réduction de prix est une sanction qui permet, selon l'article 1223 du Code civil issu de l'Ordonnance, au créancier, après mise en demeure, « *d'accepter une exécution imparfaite du contrat et de solliciter une réduction proportionnelle du prix* »[771]. Pour ce faire, il doit alors notifier sa décision au débiteur dans les meilleurs délais.

Au-delà de la mise en demeure, deux conditions de fond doivent être réunies, l'exécution du contrat doit imparfaite et la réduction du prix doit être proportionnelle. Selon l'alinéa 1er de l'article 1223 du Code civil, lorsque le créancier n'a pas payé tout ou partie du prix, il peut le réduire par notification au débiteur. Tandis que selon l'alinéa 2 de ce même texte, lorsque le créancier a déjà

[770] Rapport au Président de la République relatif à l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.

[771] C. civ., art. 1223 *(Ord. nº 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

payé le prix en totalité, soit les parties s'accordent sur la réduction du prix, soit elles ne s'accordent pas et, dans ce cas, le créancier doit la demander au juge.

Là aussi, cette sanction ne semble pas satisfaisante pour le titulaire de « données personnelles » qui souhaitent faire cesser l'atteinte portée à son encontre lorsqu'un responsable de traitement a divulgué des informations intimes à son sujet.

312. A son tour, l'exception d'inexécution est-elle une sanction adéquate ? L'exception d'inexécution représente le droit, pour une partie, de suspendre l'exécution de ses obligations tant que son cocontractant n'a pas exécuté les siennes. Ce moyen de défense est, de nos jours, réglementé à l'article 1219 du Code civil qui estime que « *Une partie peut refuser d'exécuter son obligation, alors même que celle-ci est exigible, si l'autre n'exécute pas la sienne et si cette inexécution est suffisamment grave* »[772].

A ce mécanisme, l'Ordonnance de réforme ajoute une seconde hypothèse qui est celle de l'exception pour risque d'inexécution, visée à l'article 1220 du Code civil, qui autorise une partie à suspendre l'exécution de son obligation « *dès lors qu'il est manifeste que son cocontractant ne s'exécutera pas à l'échéance* »[773]. Il s'agit donc, pour la partie concernée, d'anticiper l'inexécution future de ses obligations par son cocontractant et de limiter ainsi le préjudice qu'elle pourrait subir.

Si l'exception d'inexécution n'est soumise à aucune formalité particulière, puisqu'il n'est pas besoin de recourir au juge ou d'adresser au débiteur une mise en demeure, en revanche, l'article 1219 du Code civil impose une condition de fond puisque l'exception d'inexécution ne peut être invoquée qu'en cas d'inexécution suffisamment grave. Bien que ce critère de gravité ne soit pas défini par le Code civil, il faut entendre que l'inexécution doit être suffisamment importante au regard de l'économie du contrat. Il n'est pas nécessaire qu'elle soit

[772] C. civ., art. 1219 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

[773] C. civ., art. 1220 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

complète, mais il faut qu'elle compromette l'équilibre du contrat en affectant une obligation essentielle.

Pour résumer les effets de l'exception d'inexécution, il convient d'avoir à l'esprit qu'entre les parties, l'exception d'inexécution suspend l'exécution de la prestation de celui qui s'en prévaut. Néanmoins, le contrat est maintenu. En conséquence, si le cocontractant exécute sa prestation, l'exception est levée et le contrat devra alors être exécuté.

Là encore, l'exception d'inexécution n'apparait pas comme une sanction adéquate, cela n'apporte en rien un remède efficace à la violation de la confidentialité des « données personnelles » causée par un responsable de traitement.

313. Si les mécanismes précédemment évoqués n'apportent pas véritablement de solution intéressante pour celui ou celle qui s'estime victime d'une violation des « données personnelles » qui ont été liées à l'exécution d'un contrat, l'hypothèse de la résolution, elle, semble assez appropriée.

§2 La sanction probable

314. De toutes les sanctions précédemment évoquées, la résolution apparait, non pas comme la meilleure, mais plutôt comme la plus probable. En se mettant à la place d'une personne titulaire de données personnelles victime d'un responsable de traitement malveillant, il est aisé de comprendre qu'aucune sanction n'est en réalité complètement satisfaisante. En effet, les informations relatives au traitement sont si intimes et sensibles qu'aucune sanction ne permet de contenter et d'apaiser une personne concernée qui aurait vu ses informations dévoilées, utilisées à des fins inadéquates. Pour autant, la résolution reste la sanction la plus satisfaisante pour le contrat lorsqu'un des cocontractants n'a pas respecté ses engagements.

L'article 1224 nouveau du Code civil dispose, en ces mots, que « *La résolution résulte soit de l'application d'une clause résolutoire soit, en cas d'inexécution suffisamment grave, d'une notification du créancier au débiteur ou d'une décision de justice* »[774]. C'est au sein de ce texte, lui qui énonce les différents modes de résolution du contrat pour inexécution, que le législateur a, profitant de la réforme, choisit d'introduire la résolution unilatérale du contrat pour l'ériger au rang de principe concurrent de la résolution judiciaire ou de la clause résolutoire. Cette nouvelle rédaction se démarque de l'ancien article 1184 du Code civil et entraine un renversement de logique, lui qui énonçait que « *La résolution doit être demandée en justice* »[775].

315. Pour décrire les effets de la résolution, l'article 1229 du Code civil estime que « *La résolution met fin au contrat* »[776], soit dans les conditions prévues par la clause résolutoire, soit à la date de la réception par le débiteur de la notification faite par le créancier, soit à la date fixée par le juge ou, à défaut au jour de l'assignation en justice. Pour déterminer les effets de la résolution, il faut, selon l'article 1229 alinéa 3 du Code civil, distinguer.

---

[774] C. civ., art. 1224 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

[775] C. civ., anc. art. 1184 *(Abrogé par Ord. n° 2016-131 du 10 févr. 2016, à compter du 1er oct. 2016)*.

[776] C. civ., art. 1229 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

Si les prestations échangées ne pouvaient trouver leur utilité que par l'exécution complète du contrat résolu, la résolution entraine l'anéantissement rétroactif du contrat. Cet anéantissement rétroactif implique de remettre les choses dans leur état antérieur, autrement dit de revenir au *statu quo ante*[777].

Si les prestations échangées ont trouvé leur utilité au fur et à mesure de l'exécution réciproque du contrat, la résolution n'atteint pas les tranches déjà exécutées. Il n'y a donc pas lieu à restitution pour la période antérieure à la dernière prestation n'ayant pas reçu sa contrepartie. Il convient d'y voir un mécanisme proche de la résiliation. Il convient de préciser ici que la violation du secret sur les données est un fait qui correspond à une « inexécution suffisamment grave » au sens où l'entend l'article 1124 du Code civil pour que puisse être envisager de mettre en œuvre la résolution contractuelle dans l'hypothèse qui serait celle d'un contractant peu indélicat.

316. La résolution apparait, ainsi, comme le mécanisme le plus pertinent pour le titulaire de « données personnelles » qui s'estime victime d'une violation des informations le concernant, lesquelles ont été liées à l'exécution d'un contrat. C'est en effet la résolution qui semble protéger au mieux les personnes contre lesquelles a été violée l'obligation de confidentialité à leur égard. Dernier avantage et non des moindres, la résolution du contrat entraine la disparition de celui-ci et ouvre droit à l'établissement de la responsabilité civile délictuelle du responsable de traitement qui a violé l'utilisation des « données personnelles ». En définitive, c'est la finalité de la résolution qui en fait la sanction la plus probable et satisfaisante pour le contractant perdant, c'est-à-dire celui qui a respecté son obligation, mais dont l'autre partie ne l'a pas fait, puisque cela ouvre droit à réparation par le mécanisme de la responsabilité.

Si le contrat se voit infliger une sanction, celle de la résolution, il ne faut pas en oublier les acteurs principaux, à savoir les parties, qui en sont les victimes directes. Puisque la résolution du contrat est l'effet du manquement de l'une ou l'autre des

[777] « *Comme les choses étaient avant* ».

parties au contrat, il est logique que la responsabilité de l'une ou de l'autre des parties soit recherchée.

317. Pour en terminer avec cette présentation, celle des sanctions en nature relatives à l'inexécution du contrat, il convient d'ajouter que toutes les sanctions détaillées ci-dessus peuvent être mise en œuvre, et même se cumuler lorsqu'elles ne sont pas incompatibles, sauf en cas de force majeure, cette dernière étant caractérisée « *lorsqu'un évènement échappant au contrôle du débiteur, qui ne pouvait être raisonnablement prévu lors de la conclusion du contrat et dont les effets ne peuvent être évités par des mesures appropriées, empêche l'exécution de son obligation par le débiteur* »[778]. Si l'empêchement est définitif alors le contrat est résolu de plein droit. Confronté à l'hypothèse de la force majeure, le mécanisme de la résolution est donc très favorable pour le titulaire qui aurait vu ses « données personnelles » divulguées sans son accord, puisqu'en effet, la disparition du contrat est automatique.

[778] C. civ., art. 1218 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

CONCLUSION DU CHAPITRE 1

Donnée sensible, la donnée personnelle est sujette à certaines atteintes. Si en principe, c'est la responsabilité du responsable de traitement (et/ou du sous-traitant) qu'il convient d'engager, dans certains cas il s'agira de celle du titulaire de la donnée personnelle, contractant défaillant.

Afin de pallier ces différentes inexécutions, si les sanctions d'annulation du contrat, de réduction du prix et d'exception d'inexécution sont pour le moins envisageables, la résolution du contrat en rapport avec la donnée personnelle est l'hypothèse la plus satisfaisante pour la partie lésée.

Chapitre 2 : Les sanctions au regard du droit

318. Deux types de sanctions seront possibles lorsqu'une violation en lien avec les données personnelles est caractérisée : premièrement une sanction au regard du droit civil (Section 1), et deuxièmement une sanction au regard du droit pénal et du droit administratif (Section 2).

Section 1 : La violation en lien avec des données personnelles au regard du droit civil

Lorsqu'une atteinte aux données personnelles est caractérisée, la personne concernée peut se tourner vers le droit civil pour y trouver un soutien. Ce dernier propose, aux personnes concernées victimes de violation sur leurs données personnelles, un mécanisme de réparation (Paragraphe 1) qu'il est possible de mener à plusieurs (Paragraphe 2).

§1 Les principes de réparation et de responsabilité appliqués à une violation des données personnelles

319. Si l'inexécution des obligations portant sur les données personnelles a pour conséquence première des sanctions au regard du contrat, la logique de responsabilité entraine quant à elle des sanctions au regard du droit civil lorsque des violations en lien avec lesdites données sont constatées.

En effet, au-delà du cadre contractuel, la révélation des données en violation du Règlement général sur la protection des données est l'objet de sanctions. En ce sens, le présent règlement prévoit à l'alinéa 4 de son article 82 une réparation plus effective[779] en énonçant 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 du traitement ou du sous-traitant réparation du préjudice subi* »[780].

Dans un souci de clarté et de précision, dont l'objectif est toujours celui de renforcer la sécurité des données personnelles, le règlement UE 2016/679 expose certaines situations, non limitatives, pour lesquelles la personne concernée, victime pourra se prévaloir d'un dommage. Ainsi, ce sera le cas quand le traitement litigieux a pour conséquence de donner lieu à « *des risques pour les*

[779] *V. supra §n°53.*

[780] RGPD art. 82, *préc.*

droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de donner à caractère personnel qui est susceptible d'entrainer des dommages physiques, matériels ou un préjudice moral, en particulier : lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important (…) lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sureté connexes… »[781].

En énonçant cette multitude d'exemples, ledit règlement souhaite avertir les personnes concernées contre la diversité des violations qui peut exister à l'égard de leurs propres données personnelles. D'une part, l'exposé de ce considérant est un avertissement pour les personnes concernées et, d'autre part, il permet d'inciter les personnes concernées à s'élever contre toutes violations à l'égard de leurs données personnelles.

320. Le règlement général sur la protection des données personnelles semble donc fonder le droit à réparation de la personne concernée, celle ayant subi un dommage, en s'appuyant sur le droit de la responsabilité contractuelle, lorsqu'un contrat est en lien avec les « données personnelles ».

En droit français, il ressort de l'article 1231 nouveau du Code civil que la responsabilité contractuelle, autrement dit la responsabilité pour violation des obligations nées d'un contrat, ne peut être engagée que si trois conditions de fond

[781] RGPD consid. 75, *préc.*

sont réunies : une violation de l'obligation contractuelle, un dommage et un lien entre les deux[782].

Concernant la première condition, une distinction existe entre deux types d'obligations à savoir, les obligations de moyens et celle de résultats. L'obligation est de résultat lorsque, comme son nom l'indique, le débiteur s'est obligé à fournir un résultat au créancier. En présence d'une obligation de moyens, le débiteur ne promet pas un résultat, il promet seulement de mettre en œuvre tous les moyens que mettrait en œuvre une personne raisonnable[783], pour atteindre le résultat.

Si en matière d'obligation de résultat, il suffit de prouver que le résultat n'a pas été atteint, cette preuve ne suffit pas en matière d'obligation de moyen. Lorsque l'obligation est de moyen, la responsabilité ne pourra être engagée que s'il est possible d'établir une faute contractuelle au sens strict, entendue comme une faute dans l'exécution de l'obligation de moyens, par exemple une négligence ou une imprudence.

Rapporter aux « données personnelles », la violation de l'obligation (entendu comme une faute) peut, par exemple, trouver naissance dans l'atteinte à la vie privée d'une personne ou encore dans l'atteinte au droit à l'image d'une personne. Mais c'est aussi et surtout, le plus souvent, une atteinte au consentement de la personne qui sera constitutive d'une faute. En effet, la personne concernée aura ou non donné son consentement. Si elle ne l'a pas fait et que ses « données personnelles » sont utilisées à son insu, sans son accord, le responsable de traitement sera alors responsable pour violation d'une obligation en lien avec les « données personnelles ». Plus encore, si la personne a donné son approbation, mais seulement en partie ou seulement pour une finalité précise, et que le responsable de traitement utilise ses données à caractère personnel, là encore il y aura violation d'une obligation.

---

[782] C. civ., art. 1231 *(Ord. n° 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

[783] Anciennement « *bon père de famille* ».

Concernant le dommage, seconde condition prévue par l'article 1231 du Code civil précité, une question subsiste, celle de savoir s'il faut rapporter la preuve d'un dommage pour engager la responsabilité contractuelle de son cocontractant ? De nos jours, l'analyse classique précise que l'inexécution d'une obligation contractuelle ne peut conduire à engager la responsabilité du débiteur que si elle cause un préjudice au créancier. En ce sens, la Cour de cassation a décidé que « *des dommages intérêts ne peuvent être alloués que si le juge, au moment où il statue, constate qu'il est résulté un préjudice du manquement contractuel* »[784].

321. Une autre question peut être soulevée concernant le dommage, celle de savoir quels sont les dommages réparables, lorsque le dommage est une condition de la responsabilité contractuelle ? Il convient d'énoncer en réponse que le dommage dont le créancier peut faire état est aussi bien le dommage matériel, corporel ou encore moral. Pourtant, la responsabilité contractuelle ne donne pas lieu à application du principe de réparation intégrale du préjudice subi. En effet, aux termes de l'article 1231-3 nouveau du Code civil[785], seul le dommage prévisible lors de la formation du contrat doit être réparé[786].

Au titre des « données personnelles », le dommage qui y résulte sera celui de l'exploitation d'informations intimes sans accord de la personne concernée. L'atteinte directe à la personne pourra être caractérisée et ainsi constituer un dommage permettant l'obtention de réparation pour la personne concernée.

322. Pour en terminer avec l'étude de la responsabilité ainsi évoquée et entendue au sens de sanction par équivalent à l'inexécution du contrat, il convient de se pencher sur l'analyse de la dernière condition développé par l'article 1231 du Code civil à savoir, l'exigence du lien de causalité.

Les revendications en termes de causalité sont des exigences de bon sens. Le débiteur ne doit voir sa responsabilité engagée que si le dommage peut être mis

---

[784] Cass. civ. 3eme, 3 décembre 2003 n°15-14.072.

[785] C. civ., art. 1231-3 *(Ord. nº 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

[786] Cass. civ. 1ere, 28 avril 2011 n°10-15.056.

en relation avec la violation de l'obligation contractuelle. C'est ce qu'exprime l'article 1231-4 du Code civil lorsqu'il dispose que « *Dans le cas même ou l'inexécution du contrat résulte d'une faute lourde ou dolosive, les dommages et intérêts ne comprennent que ce qui est une suite immédiate et directe de l'inexécution* »[787]. Selon ce texte, qui n'est en réalité qu'une reprise, si ce n'est une imitation, de l'ancien article 1151 du Code civil, il ne peut y avoir allocation de dommages et intérêts que s'il existe un lien de causalité entre le préjudice causé au cocontractant et l'inexécution de l'obligation contractuelle, et ce même en présence de dol ou de faute lourde. En d'autres termes, cette constance rappelle le fait qu'il ne suffit pas, seulement, de démontrer l'existence d'un fait générateur et d'un dommage pour que le cocontractant victime soit fondé à se prévaloir d'un droit à indemnisation. Pour que l'obligation de réparation soit véritablement prise en compte, il est nécessaire d'établir une relation de cause à effet.

A ce sujet, la jurisprudence précise que le lien de causalité doit être compris selon le système de la cause adéquate[788], c'est-à-dire qu'il faut distinguer parmi toutes les causes, celle qui semble être la plus pertinente dans la réalisation du dommage. Il faut bien comprendre que dans ce système, pour que le débiteur soit responsable, il faut que l'inexécution soit vraiment la cause générique du dommage.

323. Aussi, au même titre que les régimes de réparation et de responsabilités prévues par le Code civil, le règlement général sur la protection des données instaure, à travers son article 82, un mécanisme de réparation du préjudice résultant de l'inexécution d'un contrat lorsque celui-ci porte sur les « données personnelles » de la personne concernée. Le régime de responsabilité prévu à l'article cité se démarque de la responsabilité civile contractuelle, puisque son application, sa mise en œuvre est plus générale. En effet, il s'agit ici, pour les responsables de traitement et/ou les sous-traitants de réparer, donc de dédommager, la personne concernée par le préjudice subi, lequel résulte d'une

---

[787] C. civ., art. 1231-4 *(Ord. nº 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016)*.

[788] *V. Par ex. Civ. 1re, 17 févr. 1993: JCP 1994. II. 22226, note Dorsner-Dolivet; Gaz. Pal. 1994. 1. 82, note Memmi; RTD civ. 1993. 589, obs. Jourdain*.

violation du présent règlement. Plus loin encore, le texte, précédemment énoncé, ne se contente pas de venir au secours des seules personnes concernées et de leurs données, puisqu'il étend son action à toute personne ayant subi un préjudice du fait de la violation du règlement européen. Il faut imaginer par exemple le cas d'une personne morale qui décide d'agir en cas de traitement illicite de données par un concurrent, ce qui lui porterait, naturellement, préjudice.

324. Ainsi, pour assurer une meilleure protection des personnes concernées, ou plutôt, de toutes personnes ayant subi un préjudice, à l'égard de toutes atteintes, de toutes violations, subies à l'encontre de leurs données personnelles, un mécanisme s'est peu à peu développé pour faire face aux responsables de traitements, lesquels sont toujours plus nombreux et puissants. Il sera alors question de s'intéresser à l'épanouissement de l'action de groupe appliquée aux données personnelles.

§2 Le développement de l'action de groupe en matière de données personnelles

325. Si le droit civil offre aux personnes concernées par les traitements de données des moyens juridiques pour s'assurer de la sécurité, de la protection, des données personnelles, voir même de réparation suite à une atteinte causée à celles-ci, il faut pouvoir mettre en œuvre ces moyens.

L'un des défis majeurs, en matière de données personnelles, représente le fait d'essayer d'équilibrer la relation existant entre les personnes concernées et les responsables de traitement.

Il serait déraisonnable de vouloir freiner la relation qui existe entre ces acteurs, tant cette relation est indissociable. D'une part, les personnes concernées ont, nécessairement, besoin de responsable de traitement car c'est une nécessité quotidienne pour elles d'utiliser leurs données personnelles. D'autre part, lorsque les données personnelles sont utilisées, c'est le rôle confié aux responsables de traitement de les collecter, les traiter, les conserver, en définitive d'encadrer leur utilisation.

326. Ce serait une erreur de ne s'intéresser aux responsables de traitement et du lien qui existe avec les données personnelles, seulement en dénonçant les côtés négatifs et malveillants. Pour autant, si l'interaction entre ces acteurs et les données personnelles n'est plus à prouver, il ne faut pas en occulter les dérives, lesquelles existent à cause de l'inégalité entre les personnes qui consentent à mettre à disposition leurs données personnelles et celles qui acceptent d'en user. Si par défaut ces acteurs semblent égaux, car ils ont chacun besoin l'un de l'autre, pour l'épanouissement des données personnelles, en définitive les responsables de traitement ont, malheureusement, l'ascendant du fait de leur position dominante.

Aussi, voilà pourquoi, pour s'opposer à cette position dominante, le mécanisme de l'action de groupe s'est, également, développé en matière de données

personnelles. L'intérêt d'un tel dispositif représente, pour les personnes concernées, un moyen de pouvoir s'élever contre les abus, notamment en se regroupant contre les responsables de traitements qui agissent à des fins malintentionnées, que ce soit à leur encontre ou à celle de leurs données personnelles.

327. Avant de s'intéresser à l'émergence de l'action de groupe en matière de données personnelles, il convient de revenir sur la définition de cette notion. Est une action de groupe « *l'action judiciaire diligentée par un représentant d'un groupe, désigné par la loi, afin que ledit groupe, suite au dommage de masse causé par les manquements d'un professionnel, puisse obtenir une réparation judiciaire* »[789].

Dès la définition de cette notion, il est, naturellement possible de la rapprocher avec celle de données personnelles. Plusieurs personnes concernées, victimes de violation de leurs données, peuvent s'élever contre un dommage répété causé par un responsable de traitement défaillant et malveillant, dans l'objectif d'obtenir réparation du préjudice résultant de l'atteinte aux données personnelles.

328. En matière de données personnelles, l'action de groupe a été créée par la loi du 18 novembre 2016[790] et introduite dans la loi du 6 janvier 1978[791] à travers l'article 43 ter dont le deuxième point dispose 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* ».

---

[789] S. Guinchard, C. Chainais et F. Ferrand, Procédure civile, *Droit interne et droit de l'Union européenne*, 2014, coll. Précis, Dalloz, n° 404.

[790] Loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle.

[791] Art. 43 ter, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (*Création Loi n° 2016-1547 du 18 novembre 2016 – art. 91)*.

329. L'objectif de cette action était celui de permettre aux personnes concernées victimes de manquements similaires aux obligations de protection des données personnelles, d'en demander la cessation devant la juridiction compétente. Cet objectif était assez réducteur, pour preuve en effet, le troisième point de l'article 43 ter, déjà cité, énonçait en ces mots restrictifs que « *Cette action tend exclusivement à la cessation de ce manquement* »[792].

Pour améliorer la portée et l'impact de l'action de groupe en matière de données personnelles, son champ, son programme a été élargi. Il n'est plus seulement question d'obtenir, de la part des personnes concernées touchées par une violation de leurs données, la cessation du manquement en question, il est aussi possible d'obtenir réparation des préjudices. Désormais, le second point de l'article 37 de la loi relative à l'informatique, aux fichiers et aux libertés, mise à jour, énonce que « *Lorsque plusieurs personnes physiques placées dans une situation similaire subissent un dommage ayant pour cause un manquement de même nature aux dispositions du règlement (UE) 2016/679 du 27 avril 2016 ou 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 au vue des cas individuels présentés par le demandeur, qui en informe la Commission nationale de l'informatique et des libertés* »[793] et le troisième point de ce même article d'ajouter, en tant que nouveauté bienvenue, que « *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* »[794].

Ces modifications attendues se relèvent être un soutien pour la sécurité des données personnelles dans l'objectif d'équilibrer la relation qui existe entre les

---

[792] *Ibid.*

[793] Art. 37, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Modifié par Ordonnance n° 2018-1125 du 12 décembre 2018 – art. 1).

[794] *Ibid.*

personnes concernées et les responsables de traitement. Il est aujourd'hui possible pour les personnes concernées de se concerter, de se regrouper, pour dénoncer les agissements malveillants et manquements des responsables de traitement à l'égard de leurs propres données personnelles. Bien plus que de seulement faire cesser ces atteintes, ce qui était déjà une possibilité non négligeable pour sauvegarder la protection des données personnelles, il est maintenant possible de mettre cesdits responsables de traitement face à leur responsabilité.

Le fait que la Commission nationale de l'informatique et des libertés soit informée d'une action de groupe ajoute une dimension pour le bien des données personnelles. En mettant cet organe de contrôle des données personnelles au courant des actions menées, cela ne peut que servir la cause de celles-ci et mettre en garde les responsables de traitement qui auraient de mauvaises intentions.

330. Depuis l'entrée en vigueur du règlement général de la protection des données, l'action de groupe s'y retrouve également introduite à l'article 80 dont l'intitulé concerne la « représentation des personnes concernées » en précisant ce qui suit à savoir que « *La personne concernée a le droit de mandater un organiser, une organisation ou une association à but non lucratif, qui a été valablement constitué conformément au droit d'un État membre, dont les objectifs statutaires sont d'intérêt public et est actif dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel les concernant pour qu'il introduire une réclamation en son nom, exerce en son nom les droits visés aux articles 77, 78 et 78 et exercer en son nom le droit d'obtenir réparation visé à l'article 82 lorsque le droit d'un État membre le prévoit* »[795].

Mécanisme de droit civil, l'action de groupe s'est entrepris de la question des données personnelles pour en assurer la protection. Si le règlement général de la protection des données a pour objectif de préserver les intérêts des données personnelles, l'utilisation de tel procédé, emprunté à des domaines voisins, en

[795] RGPD art. 80, *préc.*

l'espèce la procédure civile, permet de réduire l'écart existant entre les responsables de traitement d'un côté et les personnes concernées de l'autre.

331. Lorsque des violations sont constatées à l'égard de données personnelles, le droit civil fournit des mécanismes pour se protéger. C'est, toujours, dans cet esprit que le droit pénal, cette fois, apporte à son tour la pierre à l'édifice.

Section 2 : La violation en lien avec des données personnelles au regard du droit pénal et administratif

332. Selon ses propres chiffres, la Commission nationale de l'informatique et des libertés indique avoir enregistrée sur l'année 2018 « un nombre record de 11.077 plaintes »[796], soit une hausse historique du nombre de plaintes de 32 % par rapport à l'année précédente. Cette croissance, qui s'explique bien logiquement par rapport à l'entrée en vigueur du Règlement général sur la protection des données personnelles, permet de se poser toutefois une question. En effet, il est possible de se demander ce qui se passe réellement après une plainte ? Pour le dire d'une autre manière, c'est en réalité tout l'enjeu des sanctions dont il est question.

Avant de traiter ce sujet, il convient de rappeler que selon l'article 3 du règlement général sur la protection des données personnelles, le présent texte a vocation à s'appliquer « *au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union* »[797].

Aussi, en cas de non-respect des règles, en cas de violation en lien avec des « données personnelles », tout établissement, quel qu'il soit, sera alors responsable, le présent règlement ne faisant pas de distinction selon la nationalité du responsable. Ainsi, il convient d'étudier les deux types de sanctions applicables en cas de violation en lien avec des « données personnelles ».

333. Si les sanctions de la violation en lien avec les données personnelles sont d'abord et avant tout pénales (Paragraphe 1), les sanctions administratives, prescrites par l'organe de contrôle de la bonne application du présent règlement, ont également un certain pouvoir répressif (Paragraphe 2).

---

[796] URL : ttps://www.01net.com/actualites/protection-des-donnees-la-cnil-croule-sous-les-plaintes-1673768.html

[797] RGPD art. 3, *préc.*

§1 L'approche pénale et ses limites

334. Il sera, tout d'abord, pertinent d'évoquer les différentes sanctions pénales infligées en cas de violation des textes assurant la protection des « données personnelles » (A), mais aussi d'en démontrer les faiblesses (B).

A) L'apport du droit pénal à l'encontre de la protection des données personnelles en cas de violation de celles-ci

335. Cette possibilité est en effet offerte par ledit règlement à travers l'article 84 alinéa 1er, propre aux sanctions, qui énumère le fait que « *Les États membres déterminent le régime des autres sanctions applicables en cas de violations du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions sont effectives, proportionnées et dissuasives* »[798].

Voici donc un aperçu de la manière dont le droit pénal français sanctionne les violations du règlement général sur la protection des données, tout en sachant que le Code pénal était déjà muni, bien avant l'entrée en matière du règlement européen, d'une section VI propre aux différentes atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques.

336. D'après ces différents articles, sont punis d'une peine maximum de 5 ans d'emprisonnement et d'une amende pouvant aller jusqu'à 300.000 euros, le fait par les personnes responsables du traitement de :

- Procéder à celui-ci sans respecter des formalités préalables à leur mise en œuvre par la loi (article 226-16 du Code pénal)[799].

---

[798] RGPD art. 84 al. 1er, *préc.*

[799] C. pén., art. 226-16 (*L. n° 2004-801 du 6 août 2004, art. 14*).

- Procéder à ce traitement en violation de l'article 34 de la loi Informatique et Libertés relatif à l'obligation de sécurité (articles 226-17[800] et 226-17-1du Code pénal)[801].

- Collecter des données personnelles par un moyen frauduleux, déloyal ou illicite (articles 226-18 du Code pénal)[802].

- Procéder à un traitement de données concernant une personne malgré son refus, lorsque ce traitement est fait à des fins de prospection ou lorsque cette opposition est fondée sur des motifs légitimes (articles 226-18-1 du Code pénal)[803].

- Mettre ou conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaitre les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle ou à l'identité de genre de celles-ci (articles 226-19 du Code pénal)[804].

- Détourner la finalité des données personnelles (articles 226-21 du Code pénal)[805].

- Procéder à un transfert de données transfrontières contrevenant aux mesures prises par la Commission des Communautés européennes ou à l'article 70 de la loi Informatiques et Libertés (article 226-22-1 du Code pénal)[806]

---

800 C. pén., art. 226-17, *préc*.

801 C. pén., art. 226-17-1 (*L. n° 2004-801 du 6 août 2004, art. 14*).

802 C. pén., art. 226-18 (*L. n° 2004-801 du 6 août 2004, art. 14*).

803 C. pén., art. 226-18-1 (*L. n° 2004-801 du 6 août 2004, art. 14*).

804 C. pén., art. 226-19 (*L. n° 2004-801 du 6 août 2004, art. 14*).

805 C. pén., art. 226-21 (*L. n° 2004-801 du 6 août 2004, art. 14*).

806 C. pén., art. 226-22-1 (*L. n° 2004-801 du 6 août 2004, art. 14*).

Par ailleurs, l'absence d'information des personnes concernées par le traitement[807] et le non-respect de leurs droits[808] peuvent faire encourir au responsable du traitement des amendes « *prévues pour les contraventions de la cinquième classe* », d'un maximum de 1.500 euro, tel que le précisent les articles R. 625-10 et suivants du Code pénal.

337. Si le droit pénal énumère diverses sanctions applicables en cas de non-respect, donc de violation à l'égard des données personnelles, ces sanctions ne semblent pas aussi pertinentes et autoritaires qu'elles n'y paraissent.

[807] C. pén., art. R. 625-10 (*Décr. N° 2005-1309 du 20. oct. 2005)*.

[808] C. pén., art. R. 625-11 (*Décr. N° 2005-1309 du 20. oct. 2005)*.

B) La défaillance du soutien accordé par le droit pénal à l'encontre des données personnelles

338. C'est à n'en pas douter, le rôle du droit pénal à l'égard des données personnelles est, avant tout, dissuasif. En instaurant plusieurs sanctions et amendes possibles un climat de peur et de méfiance, pour celui qui souhaiterait collecter, utiliser, traiter des données personnelles avec de mauvaises intentions, semble s'installer.

Pour autant, si cette démarche peut facilement faire office de premier bouclier contre les attaques aux données personnelles, il semble que lesdites sanctions pénales ne soient pas toujours bien adaptées, amenant ainsi à renverser l'effet pourtant voulu.

Il semble, en effet, difficile d'expliquer pourquoi et comment les peines prévues par le Code pénal pour des violations à l'égard des données personnelles soient aussi élevées, pour rappel le maximum prévu étant de 5 ans de prison et de 300 000 € d'amende[809], alors que le même Code pénal prévoit par exemple, seulement, 3 ans d'emprisonnement et 45 000 € d'amende pour le cas d'un homicide involontaire[810].

339. Si les multiples atteintes causées aux données personnelles doivent pouvoir être valablement sanctionnées, dans le but de les limiter, il ne faut pas oublier que ces données-là ne sont que des fragments de la vie privée[811]. Il est assez incompréhensible, voire inquiétant, que l'atteinte aux données personnelles soit bien plus lourdement sanctionnée qu'une atteinte à la vie, même si celle-ci résulte d'une action, non souhaitée, c'est-à-dire involontaire.

---

809 *V. supra §n°335.*

810 « *Le fait de causer, dans les conditions et selon les distinctions prévues à l'article 121-3, par maladresse, imprudence, inattention, négligence ou manquement à une obligation de prudence ou de sécurité imposée par la loi ou le règlement, la mort d'autrui constitue un homicide involontaire puni de trois ans d'emprisonnement et de 45 000 € d'amende* », C. pén., art. 221-6 (*L. n° 2004-801 du 6 août 2004, art. 14*).

811 *V. supra §n°70 sur le fait que la donnée personnelle est un fragment de la personnalité.*

La différence de traitement entre ces deux types de sanctions, pour ces deux objets bien différents, d'un côté, l'atteinte à un échantillon de la vie d'une personne, de l'autre, l'atteinte directe à la vie d'une personne, va à l'encontre du souci de protection. En instaurant un plafond si élevé, cette sanction ne fait plus office de menace, mais ressemble à une peine imprononçable qui n'a plus de réel effet dissuasif[812].

En réalité il serait plus judicieux de disposer de sanction moindre mais dont l'application et l'effectivité seraient bien plus rigoureuses afin que l'effet dissuasif joue pleinement son rôle.

340. Il est à noter que la défaillance n'est pas seulement du fait du droit pénal, un manque d'ambition ou de motivation de la part des personnes concernées victimes de violation à l'égard de leurs données personnelles est également à déplorer. En effet, il semble d'une part que les personnes victimes aient peu d'intérêt à s'élever contre les responsables de traitement puisqu'il est difficile de se rendre compte du préjudice subi, d'autre part, le rapport de force entre ces deux parties est tellement déséquilibré qu'il est difficile, matériellement, financièrement, pour un titulaire de données personnelles de mener à bien une action en justice, la partie adverse faisant le plus souvent partie des leaders mondiaux dans son secteur, tel que c'est le cas pour les plateformes de réseaux sociaux sur internet.

Tant du point de vue, strictement, législatif que de celui des personnes qui peuvent mettre en œuvre le volet pénal, il semble que l'application de la sanction de la violation à l'égard des données personnelles manque de vigueur et d'effectivité.

341. Il conviendra donc, en suite, après avoir évoqué les sanctions pénales en cas de violation en lien avec des « données personnelles » de se focaliser sur les

---

[812] « *Une telle différence est surprenante, difficilement justifiable en l'absence d'atteinte aux biens ou aux personnes, et en l'absence de préjudice financier. En conséquence, ces peines ne sont jamais appliquées, à leur taux maximal : il ressort de l'étude de la jurisprudence que les amendes prononcées se chiffrent plutôt en milliers d'euros et que la prison est rarement infligée* », F. Mattatia, *RGPD et droit des données personnelles*, *Op cit*, p. 211 et 212.

différentes sanctions infligées et autorisées par ledit règlement en cas de non-respect de celui-ci par les responsables de traitement.

§2 Le recours à l'autorité de contrôle et aux sanctions administratives

342. Si en théorie le droit pénal est un soutien inconditionnel aux atteintes à la vie privée, en général, ce qui s'applique également à celles relatives aux données personnelles, en pratique les sanctions pénales sont difficiles à mettre en œuvre. Voilà pourquoi, il convient de se tourner vers d'autres acteurs qui surveillent la bonne exécution du règlement général sur la protection des données.

Pour ce faire, il convient notamment de faire un éclairage de l'article 58 dudit règlement[813] relatif aux pouvoirs conférés à l'autorité restreinte, c'est-à-dire la Commission nationale informatique et liberté.

En effet, en tant qu'autorité de contrôle, la Commission nationale de l'informatique et des libertés « *dispose du pouvoir d'adopter toutes les mesures correctrices suivantes* »[814] elle peut prononcer un rappel à l'ordre, enjoindre de mettre le traitement en conformité (y compris sous astreinte), limiter temporairement ou définitivement un traitement, suspendre les flux de données, ordonner de satisfaire aux demandes d'exercice des droits des personnes (y compris sous astreintes) ou enfin en dernier recours prononcer une amende administrative.

343. Du simple avertissement à la limitation ou suspension temporaire des traitements de données en passant par l'injonction de cesser la violation en question, l'autorité de contrôle (*cf. la Commission nationale de l'informatique et des libertés*) dispose de moyens dissuasifs et progressifs en fonction de la gravité du manquement du responsable de traitement à une des obligations du Règlement UE 2016/679.

Le dernier recours utilisé par l'autorité de contrôle pour sanctionner le non-respect du règlement est celui cité par l'article 83 de ce même texte[815]. Cet article liste les

[813] RGPD art. 58, *préc.*

[814] RGPD art. 58 2°, *préc.*

[815] RGPD art. 83, *préc.*

différentes conditions nécessaires en vue d'imposer une sanction à un organisme qui aurait violé le règlement européen. Deux types de sanctions, prévues par l'article 83 précité, peuvent être mis en exergue.

En effet, dans le souci de renforcer la protection des « données personnelles », le règlement s'est doté de sanction accrue pour atteindre ses objectifs.

Aussi, selon la gravité du dysfonctionnement constaté, une amende d'un montant de 2% du chiffre d'affaires mondial pour les entreprises ou une amende de 10 millions d'euros peut être appliquée. Pour les infractions dites plus graves telles que la mauvaise application ou le non-respect du présent règlement, une amende correspondant à 4 % du chiffre d'affaires mondial s'agissant des entreprises ou une amende de 20 millions d'euros pourra être mise en œuvre.

Il parait important de ne pas oublier d'ajouter que le cumul des sanctions administratives et pénales est possible. En effet l'article 47 alinéa 4 de la Loi n° 78-17 du 6 janvier 1978 dispose à ce titre que « *Lorsque la formation restreinte a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que l'amende administrative s'impute sur l'amende pénale qu'il prononce* »[816].

L'idée, dans le fait d'énoncer des amendes aussi élevées (tant pénales qu'administratives), est celle de faire peur aux responsables de traitement et conduire ces derniers à se mettre en conformité avec le règlement. Une sanction n'est rien d'autre qu'une « *mesure de contrainte accompagnant toute règle de droit* »[817], aussi pour faire respecter la règle il faut impressionner, comme le traduit si bien l'expression française, il faut imposer « *La peur du gendarme* ».

344. Pour terminer complètement l'analyse voici la pensée de Marie-Laure Denis, nouvelle présidente de la Commission nationale de l'informatique et des

[816] Art. 47 al. 4, Loi n°78-17 du 6 janvier 1978, *préc.*

[817] Lexique des termes juridiques, *préc.*

libertés, au sujet des sanctions en lien avec la violation en lien avec des « données personnelles », donc au sujet des conséquences de la conformité ou non au règlement général sur la protection des données personnelles.

Interrogée lors d'un entretien exclusif, la nouvelle présidente de ladite Commission fait part des volontés futures de cette institution en déclarant que « *La Cnil a volontairement fait preuve de patience et de tolérance car le RGPD est un changement profond. Mais, même s'il est entré en application depuis seulement un an, le règlement a été adopté en 2016, il y a trois ans. Je considère qu'il faut désormais faire preuve de davantage de fermeté* »[818].

345. Au demeurant, si la théorie prône la fermeté, quels sont les types de sanctions appliquées en pratique ? Pour ce faire, il convient de mentionner quelques exemples de sanctions infligées par l'autorité de contrôle sur le territoire national et sur le continent européen.

En France premièrement, il apparait que sur l'année 2018, quelque 310 contrôles ont été effectués par la Commission, ce qui a conduit, cette dernière, à prononcer 48 mises en demeure (dont 13 rendues publiques) et 11 sanctions (dont 9 pécuniaires).

A titre d'exemple, voici quelques sanctions pécuniaires infligées par la formation restreinte de la Commission nationale de l'informatique et des libertés, qui après en avoir délibéré, avait décidé, en janvier 2018 de « *prononcer une sanction pécuniaire à l'encontre de la société ETABLISSEMENTS DARTY ET FILS d'un montant de cent mille (100.00) euros* »[819] et en mai 2018 de « *prononcer à l'encontre de la société OPTICAL CENTER une sanction pécuniaire d'un*

[818] URL : https://www.latribune.fr/technos-medias/internet/rgpd-la-cnil-sera-plus-ferme-envers-les-entreprises-annonce-sa-presidente-marie-laure-denis-814287.html

[819] Délibération de la formation restreinte n° SAN-2018-001 du 08/01/2018 prononçant une sanction pécuniaire à l'encontre de la société ETABLISSEMENTS DARTY ET FILS.

montant de deux cent cinquante mille (250 000) euros »[820] ; pour les mêmes raisons, à savoir, défaut de sécurité des données sur un site internet.

A la fin de l'année 2018, au mois de décembre, la Commission avait infligé une amende à une société de transport de personnes, pour une autre raison, à savoir en l'espèce défaut de sécurité des données sur son application mobile, en énonçant « *décide, de prononcer à l'encontre de la société UBER FRANCE SAS, agissant en tant qu'établissement des sociétés UBER INC et UBER BV, une sanction pécuniaire d'un montant de quatre cent mille euros (400. 000)* »[821].

Ces trois décisions intervenues au courant de l'année 2018 représentent des sanctions pécuniaires aux sommes importantes, érigeant ainsi ces entreprises respectives comme des contres-exemples à ne pas suivre.

346. Toujours dans cet esprit dissuasif, la même Commission a infligé, en début d'année 2019, une amende record à Google d'un montant de 50 millions d'euros, reprochant à cette entreprise d'avoir « *manqué de transparence en n'informant pas de manière suffisamment claire les utilisateurs et pour n'avoir pas recueilli de manière éclairée, spécifique et sans équivoque le consentement des personnes concernées par le traitement* »[822].

Si dans le cas de Google, l'amende ne représente qu'une partie infime du chiffre d'affaires mondial de cette entreprise (environ 0,04 %) alors que règlement général sur la protection des données laisse à la Commission la possibilité d'étendre la sanction pécuniaire jusqu'à 4 %, cela représente tout de même une amende inédite servant ainsi de mise en garde au respect du devoir d'exemplarité de ces grandes enseignes internationales.

---

[820] Délibération de la formation restreinte n° SAN-2018-002 du 7 mai 2018 prononçant une sanction pécuniaire à l'encontre de la société OPTICAL CENTER.

[821] Délibération de la formation restreinte n° SAN-2018-011 du 19 décembre 2018 prononçant une sanction pécuniaire à l'encontre de la société UBER FRANCE SAS.

[822] URL : https://www.lebigdata.fr/rgpd-google-france-amende

En Europe ensuite, la Commission nationale de l'informatique et des libertés portugaise (la *Comissao Nacional de Proteceao de Dados*) avait, avant toute autre autorité de contrôle, infligé plusieurs amendes, au visa de l'article 83 du Règlement général sur la protection des données personnelles, pour un montant total de 400. 000 euros au centre hospitalier de Barreiro pour violation des principes de confidentialité des données, violation du principe de limitation d'accès aux données et pour l'incapacité de l'hôpital à garantir la confidentialité et l'intégrité des données[823].

347. Il semble qu'en définitive, si l'entrée en application du Règlement européen a demandé un effort pour les entreprises, ce qui était un temps respecté par les autorités de contrôle, la conformité à celui-ci est devenue un souci actuel majeur, et à ce titre les sanctions devraient, de jour en jour, s'alourdir en cas de non-respect envers ce dernier.

[823] URL: http://www.staub-associes.com/premiere-sanction-rgpd-portugaise/

CONCLUSION DU CHAPITRE 2

En cas de violation d'obligations en lien ave des données personnelles, c'est premièrement vers le droit commun qu'il convient de se tourner pour trouver satisfaction (sanction pénale, logique de responsabilité contractuelle ou encore action de groupe).

Pour autant, puisque ces principes de réparation connaissent quelques limites, le recours au volet administratif et aux autorités de contrôle est le bienvenu, l'effet dissuasif apportant une protection supplémentaire aux données personnelles.

CONCLUSION DU TITRE 2

348. L'inexécution des obligations portant sur les données personnelles est sanctionnée par différents mécanismes et pour plusieurs raisons.

349. Au regard du contrat d'abord, différentes sanctions, très classiques, émanent de l'inexécution de celui-ci. A celles-ci s'ajoutent les sanctions liées à la responsabilité de l'utilisateur et du titulaire des données lesquelles sont appliquées lorsque ces derniers sont défaillants.

350. Par-delà le cadre contractuel, au regard du droit commun ensuite, il est apparu que l'inexécution des obligations en violation avec les données personnelles peuvent être sanctionnées tant au plan civil que pénal et quelquefois de manière sévère.

CONCLUSION DE LA DEUXIEME PARTIE

351. Il ressort de cette deuxième partie que les contrats portant sur les données personnelles suivent le même schéma que les contrats de droit commun. Aussi l'exécution et l'inexécution sont des étapes qui font partie de la vie des contrats en lien avec les données personnelles.

352. L'exécution des contrats portant sur les données personnelles est marquée par certaines obligations en lien avec l'utilisation de la donnée personnelle quand d'autres s'attachent à la protection de celle-ci.

353. L'inexécution des obligations portant sur les données personnelles est quant à elle encadrée par différentes sanctions, tant civile que pénale, touchant le cocontractant défaillant, c'est-à-dire à la fois l'utilisateur de la donnée (responsable de traitement) et le titulaire de celle-ci (la personne concernée).

CONCLUSION GENERALE

354. La donnée personnelle est par nature une chose immatérielle profondément attachée à la personne et donc à ce titre obéit à un cadre juridique et à un régime qui en fait une « chose » juridique hors du commun.

Dès lors, s'interroger sur les contrats et les données personnelles devaient nous amener à nous demander quelle était l'influence de la donnée personnelle sur le droit du contrat, tant au regard de sa formation que de son exécution.

355. A chacune de ces étapes, depuis la naissance jusqu'à l'extinction du contrat, il est apparu que la présence de la donnée personnelle donnait un relief au contrat, soit en imposant les règles classiques liées aux éléments nécessaires à l'existence de celui-ci, soit en renforçant les mécanismes permettant de protéger le contrat ou les contractants.

356. Souvent en lien avec les libertés individuelles ou personnelles, en raison du caractère très privée des informations contenues dans les données, les contrats qui portent sur la collecte, l'utilisation ou la conservation des données personnelles, sont fortement encadrés par un dispositif législatif national, mais aussi régional, qui influe sur le contrat dont elle est un élément et dont le règlement général européen est venu apporter des précisions quelquefois superfétatoires face au droit français qui se montrait déjà très exigeant, quelquefois nouvelles ou posant une harmonie entre les pays.

C'est un élément nécessaire compte tenu du caractère souvent international des contrats portant sur les données et face au risque international de volatilité des données, qui en raison de leur caractère dématérialisé, peuvent circuler avec une facilité que la règlementation nationale ne peut pas forcément contrôler.

357. Le texte de droit européen n'est pourtant pas exempt de faiblesses ou d'imprécisions et sera surement bien en peine de protéger contre tous les risques d'utilisation illicite ou frauduleuse des données personnelles. Le règlement général sur la protection des données n'a pas la vocation ni les pouvoirs pour s'ériger seul contre les atteintes faites aux données personnelles par les responsables de traitement et anéantir ces pratiques, mais l'instauration de celui-ci fait qu'il participe, à sa manière et à son échelle, à leur protection et défense.

Si cette ambition semble ardue pour ledit règlement, gageons toutefois qu'il permettra de doter la sphère contractuelle d'une plus grande rigueur et qu'il imposera aux contractants une plus grande conscience sur les enjeux existants dans l'immixtion des données dans le contrat. L'espoir communiqué ce règlement semble passer par l'éducation des personnes concernées mais aussi celle des responsables de traitement envers la protection des données personnelles.

Fragments de la personnalité, les données personnelles sont dites sensibles puisqu'elles s'attachent à la vie privée des personnes. Ainsi, s'il est possible d'utiliser et de contracter sur ces données, il convient, à ce titre, de les préserver. Voilà alors, le rôle des mécanismes propres au droit des contrats et propres au règlement général sur la protection des données personnelles.

BIBLIOGRAPHIE

Plan

I. Ouvrages généraux : manuels, précis et traités

ALLINNE (JP.) et SOULA (M.),

Les récidivistes : Représentations et traitements de la récidive (XIXe – XXIe siècle), Pur édition, 2019, p. 288.

ANCEL (F.) et FAUVARQUE-COSSON (B.),

Le nouveau droit des contrats, Guide bilingue à l'usage des praticiens, Collection LGDJ, Edition Lextenso, 2019, 558 p.

ANDREU (L.) et THOMASSIN (N.),

Cours de droit des obligations, Amphi LMD, Éditions Gualino, 6e éd., 2021-2022, 708 p.

BELLIVIER (F.),

Droit des personnes, Domat, LGDJ, Lextenso éditions, 2e éd., 2021, 300 p.

BÉNABENT (A.),

Droit des obligations, précis Domat, LGDJ, Lextenso éditions, 19e éd., 2021, 750 p.

CABRILLAC (R.),

- *Droit des obligations*, Dalloz, 14e éd., 2020, 474 p.
- *Quel avenir pour le modèle juridique français dans le monde ?*, Economica, 2011

CARBONNIER (J.),

- *Droit civil : les biens, les obligations*, PUF, 2017, 2622 p.
- *Exorde,* dans T. Revet*, L'ordre public à la fin du XXe siècle*, Dalloz, 1996, 120 p.
- *Le Code civil*, dans P. Nora (dir.), *Les lieux de mémoire*, t. 2, La Nation, Paris, Gallimard, 1986, p. 309.

CHATRY (S.) et ROBIN (A.),

Introduction à la propriété intellectuelle, Bruylant, 2e, Collection Paradigme, 2021, n° 373.

DE MONTHOLON (C-T.),

Récits de la captivité de l'Empereur Napoléon à Sainte-Hélène, Paris, 1847, t. I, p. 40.

DE TERWANGUE (C.) et ROSIER (K.),

Le règlement général sur la protection des données (RGPD, GDPR), Larcier, 2018, 928 p.

DEBET (A.), MASSOT (J.) et METALLINOS (N.),

Informatiques et Libertés, LGDJ, Les Intégrales, vol. 10, 2015, 1296 p.

DURKHEIM (E.),

L'éducation morale, Paris : Librairie Félix Alcan, 1934.

FAUVARQUE-COSSON (B.),

La réforme du droit français des contrats, Société de législation comparée, vol. 31, 2019, 552 p.

FLUCKIGER (A.),

L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?, Pratique juridique actuelle, 2013, vol. 22, n° 6, p. 837-864.

GHESTIN (J.),

Cause de l'engagement et validité du contrat, LGDJ, 1e éd., 2006, 960 p.

L'ordre public, notion à contenu variable, en droit privé français, préc., spéc., p. 83.

L'ordre public, notion à contenu variable, en droit privé français, *in* Les notions à contenu variable en droit, Trav. du centre national de recherches de logique, Bruxelles, 1984, p. 77.

GUINCHARD (S.), CHAINAIS (C.) et FERRAND (F.),

Droit interne et droit de l'Union européenne, coll. Précis, Dalloz, 32e éd., 2014, 1600 p

GRYNBAUM (L.),

Réforme du droit des contrats : synthèse du droit français et convergence avec le droit européen, Droit de l'immatériel, Lamy Revue, n°124, Mensuel Mars 2016.

HOUTCIEFF (D.),

- *Droit des contrats*, Bruylant, Paradigme, 6e éd., 2021, 794 p.
- *Droit des contrats*, Paradigme, 6eme édition, « manuel », p. 149.

JANKÉLÉVITCH (S.),

Du consentement à l'assujettissement, dans G. Cahen (dir.), *Résister : le prix du refus*, Paris, Autrement, p. 124-138.

KANT (E.),

Critique de la raison pratique, 1788.

LARROUMET (C.) et BROS (S.),

Traité de droit civil, Les obligations, Le contrat, Economica, 10e éd., 2021, 936 p.

LATINA (M.),

L'attractivité du droit des contrats : la fonction de modèle, Blog Réforme du droit des obligations, Éditions Dalloz.

LECLERC (F.),

Droit des contrats spéciaux, 2e éd., Lextenso, LGDJ, 2012, p. 21 et s.

LEFEBVRE (J.),

Leçons de droit des biens, Éditions Ellipses, Collection « Leçons de droits », 2e éd., 2013, 320 p.

MAINGUY (D.),

Le nouveau droit francais des contrats, du régime général de la preuve et des obligations (après l'ordonnance du 10 février 2016), UMR-CNRS 5815, Dynamiques du droit, 2016.

MALAURIE (P.), AYNÈS (L.) et STOFFEL-MUNCK (P.),
Droit des obligations, LGDJ, Lextenso éditions, 10e édition, p. 345.

MARTY (G.) et RAYNAUD (P.),
Traité de droit civil, Les obligations t. 1, Les sources, 1988, Sirey, n°77.

MERCADAL (B.),
Réforme du droit des contrats : Ordonnance du 10 février 2016, Dossier pratique, Éditions Francis Lefebvre, 2016, 408 p.

MEKKI (M.),
L'intérêt général et le contrat, Contribution à une étude de la hiérarchie des intérêts en droit privé, LGDJ, 2004, 928 p.

MERLIER (P.),
Philosophie et éthique en travail social, Politiques et interventions sociales, Presses de l'EHESP, 2e éd., 2020, 188 p.

MESTRE (J.) (sous dir.),
Les principales clauses des contrats d'affaires, LGDJ, Lextenso, 2e éd., 2018, 944 p.

MOUSSERON (J-M.), MOUSSERON (P.), RAYNARD (J.) et SEUBE (J-B),
Technique contractuelle, Francis Lefebvre, 5e édition, 2017, 454 p.

ORY (P.),
Les collaborateurs : 1940-1945, Éditions du Seuil, 352 p.

PELLET (S.),
Le ''contenu licite et certain du contrat'', in *Dossier*, « *Le nouveau droit des obligations* », Droit et patr., 2016, n°258.

PENA (M.),
Les origines historiques de l'article 6 du Code civil dans R.R.J., P.U.A.M., n° XVII-49, 1992-2.

PESCHANSKI (D.),

Vichy 1940-1944 : contrôle et exclusion, Edition Complexes, 1998, 209 p.

PIGNARRE (L-F.),

Que reste-t-il des bonnes mœurs en droit des contrats ? « Presque rien ou presque tout ? », LGDJ, RDC 2005 n° 4, 343 p.

PLANIOL (M.),

La cause du contrat, Traité élémentaire de droit civil, 11e éd., LGDJ, 1931, p. 396-397.

ROSIER (K.) et DELFORGE (A.),

Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD, Editions Larcier, 2018, p. 665 et s.

SIMLER (P.),

Commentaire de la réforme du droit des contrats et des obligations, LexisNexis, 2e éd., 2018, 130 p.

STRICKLER (Y.),

Droit des biens, Edition LGDJ, Collection « Cours », LGDJ, 2017, 484 p.

TERRÉ (F.) et FENOUILLET (D.),

Droit civil : La famille, Dalloz, 8eme édition, précis, p. 17.

TERRÉ (F.), SIMLER (Ph.), LEQUETTE (Y.) et CHÉNEDÉ (F.),

Droit civil : les obligations, Dalloz, « précis », 12e éd., 2048 p.

TERRÉ (F.),

- *Pour une réforme du droit des contrats*, Dalloz, 2009.
- *Pour une réforme du droit de la responsabilité civile*, Dalloz, 2011.
- *Pour une réforme du régime général des obligations*, Dalloz, 2013.

II. Ouvrages spéciaux, Thèses et mémoires

A. Ouvrages spéciaux

BARUCH (M-O.),
Le régime de Vichy 1940-1944, Paris, Tallandier, 2017.

BOURDIEU (P.),
Ce que parler veut dire. L'économie des échanges linguistiques, Paris, Fayard, 1982, 248 p.

BOURGEOIS (M.),
Droit de la donnée : Principes théoriques et approche pratique, Éditions LexisNexis, 2017, 544 p.

COHET (F.),
Le contrat, Droit en +, PUG, 2020.

DESGENS-PASANAU (G.),
La protection des données à caractère personnel : La loi « informatique et libertés », LexisNexis, 2012, 294 p.
La protection des données personnelles : Le RGPD et la loi française du 20 juin 2018, LexisNexis, 4e éd., 2019, 345 p.

DE VILLIERS (P.),
Le jour d'après, Albin Michel, 2021, 224 p.

FENNOL-TROUSSEAU (M-P.) et HAAS (G.),
Internet et protection des données personnelles, Litec, 2000, 206 p.

FÉRAL-SCHUHL (C.),

- *Cyberdroit*, *Le droit à l'épreuve de l'internet*, Dalloz, 8e éd., 2020-2021, 1852 p.

GERARD (L.),
Les sanctions en cas de non-respect du RGPD : vers une plus grande effectivité de la protection des données à caractère personnel ?, Éditions Larcier, 16/11/2018, p. 641 et s.

GUILLAUTÉ (A.),
Mémoire sur la réformation de la police en France : Soumis au roi en 1749, Hermann.

JALBY (C.),
La police technique et scientifique, Pur édition, Collection Que sais-je, 2017, 128 p.
URL : https://francearchives.fr/fr/commemo/recueil-2014/39094

HALPERN (C.),
Une identité nationale en papier, Identité(s) : L'individu, le groupe, la société, Éditions Sciences Humaines, Collection Synthèse, 2016.

LAFFAIRE (M-L.),
Protection des données à caractère personnel : Tout sur la nouvelle loi ''informatiques et libertés'', Éditions d'Organisations, 2005, 542 p.

LE TOURNEAU (P.),
Chapitre 411 : Contrat de commerce en ligne : données de fait, in *Contrats du numérique,* éd., Dalloz référence, 2021-2022.

LEONETTI (X.),
Smartsécurité et Cyberjustice, Edition PUF, Collection Questions judiciaires, 2021.

MACÉ (G.),
Le Service de la Sureté par son ancien chef, Paris, Charpentier, 1884, p. 376 sv.

MARTIAL-BRAZ (N.) et ROCHFELD (J.),
Droit des données personnelles : les spécificités du droit français au regard du RGPD, Collection Dalloz Décryptage, Edition Dalloz, 2019, 560 p.

MATTATIA (F.),

RGPD et droit des données personnelles, Éditions Eyrolles, 5e éd., 2021, 266 p.

Traitement des données personnelles : le guide juridique, Éditions Eyrolles, 2013, 187 p.

PIAZZA (P.),

Histoire de la carte nationale d'identité, Odile Jacob, Histoire, 2004, 462 p.

Septembre 1921 : la première « carte d'identité de Français » et ses enjeux, Genèses, vol. 54 (1), 2004, pp. 76-89.

Aux origines de la police scientifique – Alphonse Bertillon, précurseur de la science du crime, Karthala édition, Collection Homme et sociétés, 2011, 383 p.

TOMBAL (T.),

Les droits de la personne concernée dans le RGPD in Le Règlement général sur la protection des données (RGPD/GDPR), Larcier, 2018, p. 448.

TOMBAL (T.) et LEDGER (M.),

Le droit à la portabilité dans les textes européens : droits distincts ou mécanisme multi-facettes ?, R.D.T.I., 2018, n° 72, p. 30.

B. Thèses et mémoires

KERLEO (J-F.),

La transparence en droit, thèse de doctorat en droit Public, Lyon lll, octobre 2012 (extrait, sans note de bas de page).

MALAURIE (P.),

Les contrats contraires à l'OP, Étude de droit civil comparé : France, Angleterre, URSS, th. Paris, 1953, n°1, p. 1.

RISPOLI (N.),

L'audit de la protection des données personnelles à l'aune du Règlement Général sur la Protection des Données, Mémoire de Msc 2 en Audit et gouvernance des organisations, Sous la direction de Monsieur Jacques Vera, Année universitaire 2016-2017, p. 13.

RENARD (S.),
L'ordre public sanitaire. Étude de droit public interne, thèse droit, Rennes, 2008.

SCHERER (E.),
La révolution numérique : Glossaire, Dalloz, 2009, 224 p.
SENNETT (R.),
Autorité, Fayard, 1982, 286 p.

III. Dictionnaires, lexiques et fascicules

A. Dictionnaires et lexiques

CABRILLAC (R.) (sous dir.),
Dictionnaire du vocabulaire juridique 2022, Paris, LexisNexis, 13e éd., 2021, 552 p.

CORNU (G.) (sous dir.),
Vocabulaire juridique, Association Henri Capitant, Paris, PUF, Quadrige, 13e éd., 2020, 1136 p.

DEBARD (T.) et GUINCHARD (S.) (sous dir.),
Lexique des termes juridiques, Dalloz, 27e éd., 2021, 1100 p.

PUIGELIER (C.),
Dictionnaire juridique, Collection Paradigme, 3e éd., 2020, 1266 p.

B. Fascicules

AUTIER (E.),
CJUE : les adresses IP « dynamiques » sont des données personnelles au sens du droit de l'Union, *Dalloz actualité*, 8 novembre 2016.

BRENNER (C.) et LEQUETTE (S.),

Acte juridique – Théorie général de l'acte juridique, *Répertoire de droit civil*, Février 2009.

CADIET (L.),

Jurisclasseur civ. Code, Lexis 360, art. 1598, fasc unique, Vente, chose pouvant être vendues, 2016.

CRICHTON (C.),

Algorithme et personnalité numérique, *Dalloz actu étudiant,* 25 avril 2019.

StopCovid : mise en demeure de la CNIL, *Dalloz actualité*, 28 juillet 2020.

Données personnelles et cases pré-cochées : toujours un défaut de consentement, *Dalloz actualité*, 01 décembre 2020.

DE GAUDEMONT (C.),

Covid-19 et loi d'urgence : état d'urgence sanitaire, *Dalloz actu étudiant*, 24 mars 2020.

DEHARO (G.),

Contrat judiciaire, *Répertoire de procédure civile*, Septembre 2017 (actualisation : Décembre 2019).

DISSAUX (N.),

Contrat : formation – Détermination des conditions, *Répertoire de droit civil*, Avril 2017 (actualisation : Mars 2021).

Contrat : formation, *Répertoire de droit civil*, Avril 2017, Avril 2017 (actualisation : Mars 2021).

Contrat : formation, *Répertoire de droit civil*, Avril 2017 (actualisation : Mars 2021)

Contrat : formation, *Répertoire de droit civil*, Avril 2017, Avril 2017 (actualisation : Mars 2021) ; V. déjà A. Weill, Connaissance du motif illicite ou immoral déterminant et exercice de l'action en nullité : in Mél. G. Marty, 1978, p. 1169.

Fiche d'orientation, Dalloz, Septembre 2020, V° Ordre public - URL : https://www-dalloz-fr.ezproxy.univ-perp.fr/documentation/Document?id=DZ/OASIS/000687

GAVANO (I.) et LE MAREC (V.),

Fuite massive de données personnelles de santé, *Dalloz actualité*, 17 mars 2021.

H (M.),

L'adresse IP est une donnée personnelle, *Dalloz actualité*, 8 décembre 2016.

LATINA (M.),

Contrat : généralités, Notion de contrat, *Répertoire de droit civil*, Mai 2017, n. 159 et 160.

MAXIMIN (N.),

La CNIL consulte sur les droits numériques des mineurs, *Dalloz actualité*, 04 mai 2020.

PICOD (Y.),

Obligations, *Répertoire de droit civil*, Juin 2017, n. 37.

PY (B.),

Secret professionnel, que n'avons-nous pas retenu de l'expérience du sida ?, *Dalloz actualité,* 26 mai 2020.

STOCLIN-MILLE (C.),

La préservation de l'ordre public dans le projet de loi confortant le respect des principes de la République, *Dalloz actualité*, 17 février 2021.

La Commission des lois du Sénat réécrit l'article 24 de la loi Sécurité globale, *Dalloz actualité*, 5 mars 2021.

ZORN (C.),

État d'urgence pour les données de santé (II) : sidep et contact covid, *Dalloz actualité*, 26 mai 2020.

IV. Articles de colloques et ouvrages collectifs

A. Articles de colloques

JOINET (L.),
Expert indépendant auprès de la Commission des droits de l'homme de l'ONU, Audition à la Commission nationale de l'Informatique et des Libertés, 8 mars 2005.

MEUNIER (S.),
RGPD : Quand devez-vous obtenir le consentement, 1er Septembre 2017.

SAUVÉ (J-M.),
La simplification du droit et de l'action administrative, Colloque organisé par le Conseil d'État et la Cour des comptes, 16 déc. 2016, reproduit sur le site du Conseil d'État.

B. Ouvrages collectifs

ROCHFLED (J.),
Contre l'hypothèse de la qualification des données en tant que biens, in A. Chaigneau et E. Netter (dir.), *Les biens numériques*, PUF, 2015, p. 221 et s.

TESTU (F-X.),
Chapitre 11 : élément du contrat - Section 3 : objet du contrat , in *Contrats d'affaires* , éd., Dalloz référence, 2010.

V. Articles de revues

ADER (B.),
« Le droit à l'information sur la justice », Questions- débats, Légispresse, Cairn info 2021/HS1 (n° 65), p. 43-46.

ARMINGAUD (C-E.),
« *Le consentement : le faux-ami des bases légales ? »*, (2019), Revue Lamy droit de l'immatériel (n° 160, 2019), p. 44-46.

BEIGNIER (B.),

- *« Pour un nouveau Code civil »*, Recueil Dalloz, 2019, p. 713 ; T. Revet, A propos de l'article de Bernard Beignier *« Pour un nouveau Code civil »,* Recueil Dalloz, 2019, p. 1011 ; B. Beignier, Réponse à Thierry Revet, *« Pour un nouveau Code civil »,* Recueil Dalloz, 2019, p. 1408.

BENABOU (V-L.),

« Entrée par effraction d'une notion juridique nouvelle et polymorphe : le contenu numérique », Dalloz IP/IT, 2017, p. 7

BIZET (T.),

« L'ambition individualiste de l'autodétermination informationnelle », International Journal of Digital and Data Law, Vol 3, 2017, p. 49-60.

CABRILLAC (R.),

« *Un nouveau Code civil ? »*, Recueil Dalloz, 2019, p. 2149.

CASTETS-RENARD (C.),

« Brève analyse du règlement général de la protection des données », Dalloz IP/IT, 2016, p. 311.

CHARPENTIER (E.),

« *Le rôle de la bonne foi dans l'élaboration de la théorie du contrat »,* RDUS (Revue de Droit de l'Université de Sherbrooke), vol., 26, n°2, 1996, p. 306.

CLUZEL-METAYER (L.),

« La datasurveillance de la Covid-19 », RDSS 2020, p. 918.

DANIS-FATÔME (A.),

« Ordre public et protection des données à caractère personne »l, AJ contrat 2019, p. 366.

DEBET (A.),
« Le consentement dans le RGPD : rôle et définition », crids, article périodiques, communication commerce électronique, n°4, 2018.

DISSAUX (N.),
« Contrat : formation - Détermination des conditions », Répertoire de droit civil, Avril 2017 (actualisation : Mars 2021), n. 158 et 159.

DEBIÈS (E.),
« Big data de santé et autodétermination informationnelle : quelle articulation possible pour une innovation protectrice des données personnelles ? », Revue française d'administration publique, vol. 167, no. 3, 2018, pp. 565-574.

DEROUDILLE (A.),
« Le secret professionnel dans le règlement général sur la protection des données (RGPD) », RFDA n° 6, Novembre-Décembre 2018, p 1112, Dalloz 1er janvier 2019.

GIJSBERS (C.),
« L'incidence des règles relatives à la nullité, à la caducité et aux restitutions », RDI 2016, p. 342.

LATINA (M.),
« Contrat : généralité », Dalloz, RTD. civ. 2017 (actualisation 2020).

LEQUETTE (S.),
La notion de contrat, RTD. civ, 2018, p. 541.

LE CLAINCHE (J.) et LE MÉTAYER (D.),
« Données personnelles, vie privée et non-discrimination : des protections complémentaires, une convergence nécessaire », RLDI févr. 2013, p. 80 s., spéc. p. 91.

JOUEN (M.),
« Négociations et obligations de confidentialité », AJCA 2016, p.275.

LAZARO (C.) et LE METAYER (D.),

« Le consentement au traitement des données personnelles : une perspective comparative sur l'autonomie du sujet », Revue juridique Thémis, 43 (3), 768-815, 2015.

LEMOULAD (J-J.), PIETTE (G.) et HAUSER (J.),

« Ordre public et bonnes mœurs », Ed. Dalloz, RDC Février 2019 (actualisation Décembre 2019).

LOISEAU (G.),

« Typologie des choses hors du commerce », RTD*Civ*., 2000, p.47.

MALLET-POUJOL (N.),

« La réforme de la loi ''informatique et libertés », Revue française d'administration publique, n°89, janvier-mars 1999, p. 49-62.

MARTIAL-BRAZ (N.),

« Le renforcement des droits de la personne concernée », Dalloz IP/IT 2017, p. 253.

MARY (L.),

« Présentation de la loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales », AJ Famille 2020, p. 384.

MAZEAUD (V.),

- *« Dossier 48 : Le Conseil Constitutionnel et la vie privée »,* Nouveaux cahiers du conseil constitutionnel, Juin 2015, p. 7-20.
- *« Présentation de la réforme du droit des contrats* », Gazette du Palais, 2016, p. 15.

MILLIOT (V.),

« Réformer les polices urbaines au siècle des Lumières : le révélateur de la mobilité », Crime, Histoire & Sociétés, vol. 10, n°1, 2006, p. 25-50.
URL : http://journals.openedition.org/chs/195 ; DOI : 10.4000/chs.195

MONTEILS-LAENG (L.),

« Perspectives antiques sur la philosophie du consentement », Tracés. Revue de Sciences humaines, n°14, 2008, p. 31-43.

MUCCHIELLI (L.),

« Criminologie, hygiénisme et eugénisme en France (1870 – 1914) : débats médicaux sur l'élimination des criminels réputés « incorrigibles », Revue d'histoire des sciences humaines, 2000, n°3, p. 57-88.

PONTIER (J-M.),

« Du danger présenté par certains chiens et des moyens d'y remédier », *JCPA 2008*, act 608.

ROCHFELD (J.),

- *« Données personnelles : quels nouveaux droits ? »*, Actualité, Statistique et société, Vol. 5, n°1, avril 2017, p. 47.
- *« Les données à caractère personnels – Les données des mineurs »,* Rép. IP/IT et communication, éd., Dalloz, 2019.

ROGUE (F.),

« Capacité et consentement au traitement de données à caractère personnel et au contrat », AJ Contrat 2019, p. 370.

SAENKO (L.),

« La (quasi-) consécration du vol d'informations », RTD com., Revue trimestrielle de droit commercial et de droit économique, Dalloz, 2017, pp. 713.

SERINET (Y-M.),

« La constatation de la nullité par les parties : une entorse limitée au caractère judiciaire de la nullité », JCP 2016, p 845. (P. Lipinski, *La conversion des actes juridiques*, RRJ 2002/3, p. 1 – A. Boujeka, *La conversion par réduction, contribution à l'étude des nullités des actes juridiques formels*, RTD com. 2002. 223).

TERRIER (E.),
« Responsabilité medicale, in Responsabilité civile», Encyclopédie - Répertoire civil, Dalloz, 2020, 104 p.

VITALIS (A.),
« Informatique et libertés : une histoire de trente ans », Hermès, La Revue, 2009/1, n°53, p. 137 à 143.

VI. Sources

A. Sources nationales

Adresse aux français du Président de la République Emmanuel Macron, 16 mars 2020, Élysée.

Adresse aux français du Président de la République Emmanuel Macron, 24 novembre 2020, Élysée.

Arrêté du 27 juin 1989 relatif à l'enrichissement du vocabulaire de l'informatique.

Arrêté du 9 octobre 2020 modifiant l'arrêté du 10 juillet 2020 prescrivant les mesures générales nécessaires pour faire face à l'épidémie de covid-19 dans les territoires sortis de l'état d'urgence sanitaire et dans ceux où il a été prorogé.

Amendement n°92 rectifié au texte n° 20192020-483, Après l'article 11 (Adopté), Protection des victimes de violences conjugales, M. Mercier.

Avis du Haut Conseil de la santé publique relatif à un contrôle d'accès par prise de température dans la préparation de la phase de déconfinement en lien avec l'épidémie à Covid-19, 28 avril 2020.

Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

Conclusions du commissaire du Gouvernement sur CE, sect. 20 déc. 1957, Sté nationale d'éditions cinématographiques, *Lebon*702.

Décision n° MED 2019-035 du 31 décembre 2019 mettant en demeure la société ELECTRICITE DE FRANCE (EDF).

Décision n° MED-2020-015 du 15 juillet mettant en demeure le ministère des solidarités et de la santé.

Délibération 97-008 du 04 février 1997.

Délibération de la formation restreinte n° SAN-2018-001 du 08/01/2018 prononçant une sanction pécuniaire à l'encontre de la société ETABLISSEMENTS DARTY ET FILS.

Délibération de la formation restreinte n° SAN-2018-002 du 7 mai 2018 prononçant une sanction pécuniaire à l'encontre de la société OPTICAL CENTER.

Délibération de la formation restreinte n° SAN-2018-011 du 19 décembre 2018 prononçant une sanction pécuniaire à l'encontre de la société UBER FRANCE SAS.

Délibération de la formation restreinte n° SAN-2021-003 du 12 janvier 2021 concernant le ministère de l'intérieur.

Discours du Président Emmanuel Macron pour le 30e anniversaire de la Convention internationale des droits de l'enfant, 20 novembre 2019.

Groupe 29, *Lignes directrices relatives au droit à la portabilité des données*, WP 242 rev.01, 5 avril 2017, p. 4.

Groupe 29, *Avis 4/2007 sur le concept de données à caractère personnel*, WP 136, 20 juin 2021, p. 3.

Groupe 29, *Groupe de travail « article 29 », Lignes directrices sur la transparence au sens du règlement (UE) 2016/679*, WP 259 rev.01, 10 avril 2018, p. 7.

Protocole national pour assurer la santé et la sécurité des salariés en entreprise face à l'épidémie de Covid-19, 31 aout 2020.

P. Catala, *Présentation générale de l'avant-projet, Avant-projet de réforme du droit des obligations et de la prescription*, Rapport à Monsieur Pascal Clément, Garde des Sceaux, Ministre de la Justice, 22 Septembre 2005, p. 2.

P. Catala, *Avant-projet de réforme du droit des obligations et de la prescription*, La Documentation française, 2006.

Rapport au Président de la République relatif à l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.

Rapport du Conseil national du numérique, Identités numériques : Clés de voute de la citoyenneté numérique, Juin 2020, p.14.

B. Sources internet

URL : ttps://www.01net.com/actualites/protection-des-donnees-la-cnil-croule-sous-les-plaintes-1673768.html

URL : https://actu.dalloz-etudiant.fr/a-la-une/article/suppression-de-la-cause-reforme-du-droit-des-contrats-du-regime-general-et-de-la-preuve-des-obligations

URL : https://www.alliancepresse.fr/actualite/loi-sur-la-securite-globale/

URL : https://www.amnesty.fr/liberte-d-expression/actualites/gafa-gestion-des-donnees-personnelles

URL : https://www.avocats-mathias.com/propriete-intellectuelle/algorithmes-quelle-protection

URL : https://www.beuc.eu/publications/beuc-files-complaint-against-tiktok-multiple-eu-consumer-law-breaches/html

URL : https://www.bfmtv.com/police-justice/il-faut-proteger-ceux-qui-nous-protegent-le-depute-sylvain-maillard-appelle-a-armer-la-police-municipale-parisienne_AV-202011170126.html
URL : https://www.capital.fr/economie-politique/et-si-demain-vous-vendiez-vos-donnees-personnelles-a-facebook-1268001
URL : https://carlpepin.com/2010/09/07/la-bataille-de-france-1940/
URL : https://christian-buhlmann.com/pourquoi-les-gafa-sinteressent-ils-tant-a-vos-donnees-personnelles/
URL : https://www.cnil.fr/fr/ce-que-change-la-loi-pour-une-republique-numerique-pour-la-protection-des-donnees-personnelles
URL : https://www.cnil.fr/fr/cnil-direct/question/quest-ce-quun-tiers-autorise
URL : https://www.cnil.fr/fr/cnil-direct/question/une-donnee-caractere-personnel-cest-quoi
URL : https://www.cnil.fr/fr/comment-reagir-face-une-usurpation -didentite
URL : https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes
URL : https://www.cnil.fr//fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-données-personnelles-par-les-employeurs
URL : https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant
URL : https://www.cnil.fr/fr/definition/accountability
URL : https://www.cnil.fr/fr/definition/donnee-sensible
URL : https://www.cnil.fr/fr/edf-et-engie-mises-en-demeure-pour-non-respect-de-certaines-conditions-de-recueil-du-consentement
URL : https://www.cnil.fr/fr/la-liceite-du-traitement-lessentiel-sur-les-bases-legales-prevues-par-le-rgpd
URL : https://www.cnil.fr//fr/la-plateforme-des-donnees-de-sante-health-data-hub
URL : https://www.cnil.fr/fr/la-violation-du-trimestre-attaque-par-credential-stuffing-sur-un-site-web
URL : https://www.cnil.fr/fr/le-droit-dacces-connaitre-les-donnees-quun-organisme-detient-sur-vous
URL : https://www.cnil.fr/fr/publicite-ciblee-en-ligne-quels-enjeux-pour-la-protection-des-donnees-personnelles

URL : https://www.cnil.fr/fr/quelles-formalites-pour-les-traitements-de-donnees-de-sante-caractere-personnel
URL : https://www.cnil.fr/fr/quelles-thematiques-prioritaires-et-quelle-strategie-de-controle-pour-2018
URL : https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on
URL : https://www.cnil.fr/fr/securite-informatique-sensibiliser-les-utilisateurs
URL : https://www.cnil.fr/sites/default/files/atoms/files/guide_tiers_autorises.pdf
URL : https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf
URL : https://www.cnil.fr/sites/default/files/atoms/files/travail-vie_privee.pdf
URL : https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp136_fr.pdf
URL : https://comarketing-news.fr/rgpd-user-loser/
URL : https://www.conseil-national.medecin.fr/medecin/devoirs-droits/serment-dhippocrate
URL : https://defenseurdesdroits.fr/fr/communique-de-presse/2020/11/proposition-de-loi-securite-globale-lalerte-de-la-defenseure-des-droits
URL : https://www.delsolavocats.com/Comment-determiner-les-bases-legales-de-ses-traitements
URL : https://www.dictionnaire-academie.fr/article/A9C3120
URL : https://www.dictionnaire-academie.fr/article/A9D3040
URL : https://www.dictionnaire-juridique.com/definition/ordre-public.php
URL : https://www.dictionnaire-juridique.com/definition/rgpd.php
URL : http://dictionnaire.sensagent.leparisien.fr/données%20personnelles/fr-fr/
URL : ttps://www.digitemis.com/blog/rgpd-quelle-base-juridique-pour-vos-traitements-de-donnees-a-caractere-personnel/
URL : https://www.donneespersonnelles.fr/3-registres-rgpd-devez-mettre-place
URL : https://www.donneespersonnelles.fr/consentement-rgpd-valable
URL : https://www.droit-travail-france.fr/processus-recrutement.php
URL : https://www.e-enfance.org/les-risques-sur-internet
URL : https://www.eff.org/fr/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy
URL : https://www.efl.fr/actualites/social/contrat-de-travail/details.html?ref=f0a3c09fb-d3d8-4a50-8a6a-89537f997871
URL :https://ww.elysee.fr/admin/upload/default/0001/09/9cbaf53e3475d20381db6c0959e00e19d72aa.pdf

URL : ttps://www.elysee.fr/emmanuel-macron/2017/10/18/discours-du-president-de-la-republique-emmanuel-macron-devant-les-forces-de-securite-interieure
URL : https://www.elysee.fr/emmanuel-macron/2020/12/01/tech-for-good-plus-de-75-leaders-sengagent
URL : https://esante.gouv.fr/labels-certifications/hds/certification-des-hebergeurs-de-donnees-de-sante
URL: https://escaramozzino.legal/2019/05/29/rgpd-sante/
URL : http://espacehgfauthoux.e-monsite.com/medias/files/lecon-n-5-la-surete-un-droit-de-l-homme.pdf
URL : https://www.europe1.fr/emissions/linterview-politique-de-8h20/gerald-darmanin-assure-que-les-citoyens-pourront-toujours-filmer-les-operations-de-police-4006392
URL : https://factuel.afp.com/non-une-loi-de-2002-sur-le-consentement-des-patients-ne-permet-pas-deviter-les-vaccins-obligatoires
URL : https://fr.adforum.com/agency/9673/creative-work/34588678/ce-quils-regardent-ca-nous-regarde-tous/csa
URL : https://www.francetvinfo.fr/faits-divers/police/proposition-de-loi-securite-globale-il-n-y-a-aucune-atteinte-liberticide-au-droit-et-a-la-loi-de-la-presse-assure-le-syndicat-alliance-police_4184543.html
URL : https://www.francetvinfo.fr/replay-radio/8h30-fauvelle-dely/deconfinement-commerces-fermes-securite-globale-le-8h30-franceinfo-de-gabriel-attal_4170583.html
URL : https://www.ft.com/content/0f76f05e-d165-11e8-9a3c-5d5eac8f1ab4
URL : http://www.gazette-sante-social.fr/48652/la-protection-des-donnees-de-sante-apres-le-rgpd
URL : https://www.haas-avocats.com/actualite-juridique/justice-precise-statut-hebergeur-internet-procedure-suivre-engager-responsabilite/
URL : https://halshs.archives-ouvertes.fr/halshs-01201761/document
URL : https://www.ladn.eu/tech-a-suivre/christopher-wylie-cambridge-analytica-menaces-democraties/
URL : https://la-philosophie.com/le-stoicisme
URL : https://larevue.squirepattonboggs.com/messages-personnels-des-salaries-la-jurisprudence-nikon-n-est-pas-tout-a-fait-morte_a2857.html
URL : https://www.larousse.fr/dictionnaires/francais/personnel/59814?q=personnelle#59449
URL : https://www.larousse.fr/infos/confidentialite

URL : https://www.latribune.fr/technos-medias/internet/rgpd-la-cnil-sera-plus-ferme-envers-les-entreprises-annonce-sa-presidente-marie-laure-denis-814287.html
URL : https://www.lebigdata.fr/facebook-donnees-reseau-democratie
URL : https://www.lebigdata.fr/rgpd-google-france-amende
URL : https://www.lefigaro.fr/actualite-france/2016/10/11/01016-20161011ARTFIG00245-eric-ciotti-proteger-ceux-qui-nous-protegent.php
URL : https://www.lefigaro.fr/secteur/high-tech/le-royaume-uni-ne-controlera-finalement-pas-l-identite-des-usagers-de-sites-pornographiques-20191017
URL : https://www.legavox.fr/blog/lajurisprudence/solus-consensus-obligat-consentement-oblige-19079.htm
URL : https://www.lemonde.fr/idees/article/2020/11/10/l-article-24-de-la-future-loi-securite-globale-menace-la-liberte-d-informer-alertent-des-societes-de-journalistes_6059188_3232.html
URL : https://www.lemonde.fr/pixels/article/2018/04/04/cambridge-analytica-87-millions-de-comptes-facebook-concernes_5280752_4408996.html
URL : https://www.lemonde.fr/societe/article/2020/11/04/loi-de-securite-globale-une-proposition-pour-limiter-la-captation-d-images-sur-le-terrain_6058525_3224.html
URL : https://www.lemondeinformatique.fr/actualites/lire-apple-cisco-et-microsoft-reclament-un-rgpd-a-l-americaine-74214.html
URL : https://www.marianne.net/agora/humeurs/face-aux-gafa-nos-donnees-sont-notre-liberte
URL : https://marketoonist.com/2019/05/data-privacy-consent-fatigue-and-gdpr.htmlURL: https://www.mysih.fr/hds-de-lagrement-a-la-certification/
URL : https://www.nextinpact.com/article/28047/106168-le-rgpd-explique-ligne-par-ligne-articles-24-a-50
URL : https://www.nytimes.com/1914/02/15/archives/alphonse-bertillon.html
URL: https://www.pre-plainte-en-ligne.gouv.fr
URL : https://www.quechoisir.org/action-ufc-que-choisir-tiktok-depot-d-une-plainte-europeenne-contre-l-application-n88258/
URL : https://www.rtl.fr/actu/politique/les-gafa-s-engagent-a-etre-plus-vertueux-une-victoire-pour-macron-7800932946
URL : https://www.senat.fr/amendements/2019-2020/483/Amdt_92.html
URL : https://www.senat.fr/lc/lc62/lc621.html
URL : https://www.senat.fr/rap/r04-439/r04-4394.html

URL : https://www.senat.fr/rap/r04-439/r04-4394.html#fn44
URL : https://www.senat.fr/rap/r04-439/r04-4394.html#fn46
URL : https://siecledigital.fr/2018/03/23/cambridge-analytica-tout-comprendre-sur-la-plus-grande-crise-de-lhistoire-de-facebook/
URL : http://www.slate.fr/story/198715/vaccination-covid-19-maladie-alzheimer-consentement-refuser
URL: http://www.staub-associes.com/premiere-sanction-rgpd-portugaise/
URL :https://www.svp.com/article/algorithme-et-data-opportunite-et-danger-pour-le-recrutement-100010488
URL : http://time.com/collection/davos-2019/5502591/tim-cook-data-privacy/
URL : https://twitter.com/benjaminhue/status/1272547570129285122
URL : https://twitter.com/i/status/1328594706599653386
URL : https://twitter.com/JeanMichelMIS/status/1272552939396239360
URL : https://www.un.org/fr/universal-declaration-human-rights/
URL : https://www.vie-publique.fr/loi/277157-loi-pour-une-securite-globale-preservant-les-libertes
URL : https://www.village-justice.com/articles/accountability-rgpd-liste-des-documents-contenus-dans-dossier-conformite,33433.html
URL : https://www.village-justice.com/articles/consentement-valide-sens-rgpd,30428.html
URL : https://www.village-justice.com/articles/hebergement-donnee-sante-rgpd,30355.html#XIqQuURc0u2xZ8S9.99
URL : ttps://www.village-justice.com/articles/Hebergeur-editeur-hebergeur-editeur,16097.html
URL : https://www.village-justice.com/articles/les-nouvelles-obligations-employeur-matiere-protection-des-donnees-personnelles,28756.html
URL : https://www.village-justice.com/articles/rgpd-donnees-consentement-des-salaries-est-pas-necessaire-pertinent,30337.html
URL : www.village-justice.com/articles/rgpd-responsabilite-sous-traitant-peut-plus-etre-evitee,38225.html
URL : https://www.village-justice.com/articles/utilisation-ordinateur-professionnel-cedh-valide-jurisprudence-francaise,28375.html
URL : https://youtube.com/watch?v=sZ12bUTZXDw
URL : https://www.youtube.com/watch?v=uII6Ld4h8ik

URL : https://www.cnil.fr/fr/cnil-direct/question/la-cnil-cest-quoi
URL:https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52018DC0043&from=FR

C. Sources médiatiques

BAZOT (A.), Président directeur de l'UFC-Que Choisir, Source : FR 3 – 19/20, Edition nationale, Journal télévisé, 27 juin 2013.

BARREIRO (N.),
Affaire Snowden : révélations, demande d'asile… ce qu'il faut savoir, RTL, 16 septembre 2019.

BOUCHER (P.),
« SAFARI » ou la chasse aux Français, Le Monde, 21 mars 1974, p. 9.
URL : https://www.cnil.fr/sites/default/files/atoms/files/le_monde_0.pdf
URL : https://www.lemonde.fr/archives/article/1974/03/21/une-division-de-l-informatique-est-creee-a-la-chancellerie-safari-ou-la-chasse-aux-francais_3086610_1819218.html?xtmc=safari&xtcr=1274

CHANDY (L.), (Directeur des données, de la recherche et des politiques de l'UNICEF), *Plus de 175 000 enfants s'exposent à de nombreux risques sur internet chaque jour*, publié le 05 février 2018.

COMBLEZ (S.),
Rapport annuel e-Enfance, 2019, p.16.

CONERARDY (D.) et RAMEL (A.),
RGPD et consentement, un malentendu handicapant pour les acteurs publics, Le courrier des maires – n° 335-336, Juin-Juillet 2019, p. 36.

FIELDING (R.), *What the GDPR does – and doesn't – say about consent*, Miss IG Geek Blog, Privacy and information geek for hire, 31 Mai 2017.

MBIDA (A.), *L'intelligence artificielle pour vérifier l'âge sur Internet*, L'innovation du jour, Chronique de l'émission Europe Matin – 5h-7h, Diffusée le Jeudi 14 novembre 2019.

MACASKILL (E.) et HERN (A.),
Edward Snowden, The Guardian, Interview, 4 juin 2018.

MERCIER (M.), L'interview « Savoir comprendre », RMC, Bourdin Direct (6h-9h), Diffusée le 11 juin 2020.

PEIGNÉ (J.) interviewé par Thomas Saint-Cricq, AFP France, *Non, une loi de 2002 sur le consentement des patients ne permet pas d'éviter les vaccins obligatoires*, 2020.

PUYBAREAU (B.),
Les révélations d'Edward Snowden : de l'indignation à la légalisation des pratiques de surveillance, Institut Open Diplomacy, 4 juin 2020.

TOUFFAIT (A.),
Communication à l'Académie des sciences morales et politiques, 9 avril 1973.

UNTERSINGER (M.),
Ce que les « révélations Snowden » ont changé depuis 2013, Le Monde, 13 septembre 2019.

Propos recueillis le 12 juin à Lyon par L. Rigier et V. Benais.
URL : https://france3-regions.francetvinfo.fr/auvergne-rhone-alpes/rhone/lyon/lyon-cedric-villani-eclaire-notre-lanterne-intelligence-artificielle-1494023.html

Enquête de l'Ifop pour CAM4.fr auprès des jeunes âgés de 15 à 24 ans, Octobre 2013.

Étude OpinionWay pour 20 Minutes administrée en ligne entre le 03 et le 04 avril, 1179 répondants représentatifs des 18-30 ans en France selon la méthode des quotas – Vague 51.

Observatoire des comportements de consommation, *La collecte de données personnelles sur les sites de e-commerce*, étude complète de Mai 2018, Odoxa – Emakina.

G. Le Grand, secrétaire adjoint de la CNIL, Source : FR 3 – 19/20, Edition nationale, Journal télévisé, 27 juin 2013.

INDEX

TABLE DES MATIÈRES