UNIVERSITÉ PARIS II
PANTHÉON-ASSAS

ÉCOLE DOCTORALE DE DROIT PRIVÉ

L'EFFECTIVITÉ DE LA PROTECTION DES PERSONNES PAR LE DROIT DES DONNÉES À CARACTÈRE PERSONNEL

Thèse pour le doctorat en droit
présentée et soutenue publiquement
le 7 décembre 2020
par

Suzanne Vergnolle

sous la direction de
Monsieur Jérôme Passa
Professeur à l'Université Panthéon-Assas (Paris II)

Membres du jury

Madame Valérie-Laure Benabou
Professeur à l'Université Versailles Saint-Quentin-en-Yvelines

Monsieur Thibault Douville
Professeur à l'Université Caen Normandie, *rapporteur*

Madame Nathalie Martial-Braz
Professeur à l'Université René Descartes (Paris V), *rapporteur*

Madame Judith Rochfeld
Professeur à l'Université Paris Panthéon-Sorbonne (Paris I)

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

REMERCIEMENTS

Mes premiers remerciements s'adressent au Professeur Jérôme Passa, pour la confiance qu'il m'a accordée et la rigueur dont il a toujours fait preuve, et sans qui cette thèse n'aurait pu voir le jour.

Je remercie également les Professeurs Valérie-Laure Benabou, Thibault Douville, Nathalie Martial-Braz et Judith Rochfeld, qui m'ont fait l'honneur d'accepter de lire et de juger ce travail.

Doit également être remercié chaque enseignant qui a nourri cette réflexion et a su trouver les mots d'encouragement pour mener à bien ce travail.

Mes sincères remerciements s'adressent ensuite à ma famille : à Frédéric, pour sa présence affectueuse et stimulante ; à ma mère, pour son soutien aimant dès la première heure ; à mon père, à mes frères et à ma belle-sœur qui m'ont aidée, chacun à leur manière, à finaliser ce travail.

Ma gratitude se dirige également vers toutes les personnes qui ont consacré une partie de leur temps à la relecture et à la finalisation de ce travail. Si aucun mot n'est suffisant pour leur exprimer ma reconnaissance, qu'ils sachent que je n'oublierai pas la place que chacun d'eux occupe dans ces pages.

À Claude, dont le stylo n'a jamais manqué d'encre ; à Nicolas, pour son accompagnement averti et toujours chaleureux ; à Emmanuel, pour son avis éclairé et ses précieuses remarques ; à Antoine, dont la sagacité m'impressionne encore.

À Benjamin, Charles-Édouard, Clément, Claire-Marie, Jonathan, Julie, Julien B., Maxime C. et Suzel pour leur bienveillance, leur amitié et leurs conseils.

À toute l'équipe d'Etalab, et particulièrement à Henri Verdier, pour ces deux riches années passées ensemble.

À Peter Swire, qui a donné vie à mes recherches de droit américain.
À la Commission Fulbright et à la Fondation Georges Lurcy pour la confiance accordée et le soutien fourni pour mener à bien mes recherches aux États-Unis.

Aux agents de la CNIL, des ministères, aux membres des associations et aux avocats qui m'ont aidée à mieux cerner la pratique du droit des données personnelles.

Enfin, mes remerciements s'adressent à mes amis fidèles, et notamment aux membres du Laboratoire de droit civil, pour leurs présences, leurs rires et leurs conseils attentionnés.

LISTE DES ABRÉVIATIONS FRÉQUEMMENT UTILISÉES

AJ	*Actualité juridique*
AJDA	*L'Actualité juridique : Droit administratif*
al.	alinéa
art.	article
Bull. civ.	*Bulletin* des arrêts de la Cour de cassation, chambres civiles
Bull. crim.	*Bulletin* des arrêts de la Cour de cassation, chambre criminelle
c.	contre
CA	cour d'appel
CAA	cour administrative d'appel
Cass. Ass. plén.	Assemblée plénière de la Cour de cassation
Cass. civ.	Chambre civile de la Cour de cassation
(1^{re}, 2^{e}, 3^{e})	(première, deuxième, troisième)
Cass. com.	Chambre commerciale de la Cour de cassation
Cass. crim.	Chambre criminelle de la Cour de cassation
Cass. soc.	Chambre sociale de la Cour de cassation
CCC	*Contrats Concurrence Consommation*
CCE	*Communication Commerce électronique*
CE Ass.	Conseil d'État statuant en assemblée du contentieux
CE Sec.	Conseil d'État section
CEDH	Cour européenne des droits de l'homme
CEPD	Comité européen de la protection des données
CESDH	Convention de sauvegarde des droits de l'homme et des libertés fondamentales
ch.	chambre
chron.	chronique
CJCE	Cour de justice des communautés européennes
CJUE	Cour de justice de l'Union européenne
CNIL	Commission nationale de l'informatique et des libertés
coll.	collection
comm.	commentaire
comp.	comparaison
cons.	considérant
Cons. const.	Conseil constitutionnel
D.	*Recueil Dalloz*
DC	contrôle de constitutionnalité des normes
dir.	sous la direction de
doctr.	doctrine
Dr et pat.	*Droit et patrimoine*
Dr. Fam.	*Droit de la famille*
Dr. pén.	*Droit pénal*
éd.	édition
et al.	*et alius*
FTC	Federal Trade Commission
G29	Groupe de l'article 29 de la directive 95/46
Gaz. Pal.	*Gazette du palais*
JCl.	*Encyclopédies JurisClasseur*
JCP	*JurisClasseur périodique (Semaine juridique)*

JOCE	*Journal officiel des communautés européennes*
JORF	*Journal officiel de la République française*
JOUE	*Journal officiel de l'Union européenne*
Lebon	Recueil des décisions du Conseil d'État, statuant au contentieux
Lebon T.	Tables du recueil des décisions du Conseil d'État, statuant au contentieux
LPA	*Les petites affiches*
NBP	non publié au *Bulletin* des arrêts de la Cour de cassation
n°	numéro
not.	notamment
obs.	observations
p.	page(s)
préc.	précité
Pub. L.	Public law
QPC	question prioritaire de constitutionnalité
RDC	*Revue des contrats*
RDP	*Revue du droit public*
réf.	référés
Rép. civ.	*Encyclopédie* Dalloz, *Répertoire de droit civil*
Rép. com.	*Encyclopédie* Dalloz, *Répertoire de droit commercial*
Rép. cont. adm.	*Encyclopédie* Dalloz, *Répertoire de contentieux administratif*
Rép. eur.	*Encyclopédie* Dalloz, *Répertoire de droit européen*
Rép. int.	*Encyclopédie* Dalloz, *Répertoire de droit international*
Rép. pén.	*Encyclopédie* Dalloz, *Répertoire de droit pénal et de procédure pénale*
Rép. proc. civ.	*Encyclopédie* Dalloz, *Répertoire de procédure civile*
Rép. resp.	*Encyclopédie* Dalloz, *Répertoire de la responsabilité de la puissance publique*
Rép. soc.	*Encyclopédie* Dalloz, *Répertoire de droit des sociétés*
Rép. trav.	*Encyclopédie* Dalloz, *Répertoire de droit du travail*
RFDA	*Revue française de droit administratif*
RID comp.	*Revue internationale de droit comparé*
RLDC	*Revue Lamy droit civil*
RLDI	*Revue Lamy droit de l'immatériel*
RSC	*Revue de science criminelle et de droit pénal comparé*
RTD civ.	*Revue trimestrielle de droit civil*
RTD com.	*Revue trimestrielle de droit commercial*
RTD eur.	*Revue trimestrielle de droit européen*
RUE	*Revue de l'Union européenne*
s.	et suivants
spéc.	spécialement
t.	tome
TGI	tribunal de grande instance
th.	thèse
trad.	traduction
U.S.	*United States Reports*
USC	United States Code
v.	voir
V°	*verbo*
vol.	volume

PLAN SOMMAIRE*

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

« Ma essendo l'intento mio scrivere cosa utile a chi l'intende, m'è parso più conveniente andare dietro alla verità effettuale della cosa, che a l'immaginazione d'essa, & molti si sono immaginati. »

« *Dans le dessein que j'ai d'écrire des choses utiles pour celui qui me lira, j'ai cru plus convenable d'exposer la vérité telle qu'elle est en effet, et non d'après ce que l'on s'imagine.* »

Machiavel, Le Prince

INTRODUCTION

1. Des craintes. En novembre 1974, le conseiller d'État Bernard Tricot était chargé d'identifier les risques liés à l'usage de l'informatique[1] et de proposer une réglementation sur les traitements automatisés de données[2]. L'une des premières phrases de son rapport révèle que la commission qu'il dirigeait a entendu exprimer, dans ses enquêtes et ses consultations, « des craintes pour l'avenir, mais quand elle a recherché des cas actuels et précis d'atteintes portées aux libertés par le recours à l'informatique, elle n'en a constaté que peu »[3]. Il en ressort qu'en dépit des craintes, les atteintes effectives aux personnes étaient peu nombreuses ou, en tout cas, difficiles à déceler. Cette phrase résume peut-être l'une des principales difficultés du droit des données personnelles : d'innombrables traitements, une quantité exponentielle de données, des risques certains pour les libertés, mais des atteintes dont l'ampleur échappe souvent à la perception. Assurément, depuis la publication de ce rapport, la réalité des risques s'est amplifiée et les scandales se sont multipliés[4]. La réalisation de ces craintes s'explique notamment par l'avènement d'une société de données.

2. Une société de données. L'informatique puis la mise en réseau des ordinateurs ont décuplé le nombre de données personnelles collectées et les risques d'atteintes à la vie privée des personnes. Il n'est plus beaucoup de gestes quotidiens, d'achats, de déplacements, de décisions personnelles ou professionnelles qui ne soient pas

---

[1] L'informatique est entendue largement comme la « science du traitement rationnel et automatique de l'information ; l'ensemble des applications de cette science », *Dictionnaire de l'Académie française*, 9e éd., *Vo* « Informatique », sens 1.

[2] Décret no 74-938 du 8 novembre 1974 portant création de la commission informatique et libertés, *JORF* 13 nov. 1974, no 265, p. 11403. L'article premier de ce texte chargeait la commission de proposer au Gouvernement « des mesures tendant à garantir que le développement de l'informatique dans les secteurs public, semi-public et privé se réalisera dans le respect de la vie privée, des libertés individuelles et des libertés publiques ». Le « rapport Tricot », dont la qualité est unanimement reconnue, a amplement inspiré les principes retenus dans la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* 7 janv. 1978, no 6, p. 227.

[3] B. Tricot, « Rapport de la commission Informatique et libertés », La Documentation française, 1975, p. 11.

[4] Les derniers scandales ont notamment révélé l'ampleur de la surveillance mise en œuvre par le renseignement américain (pour un bref résumé des révélations d'Edward Snowden, v. M. Untersinger, « Ce que les "révélations Snowden" ont changé depuis 2013 », *Le Monde* 13 sept. 2019), ainsi que la manipulation du public en lien avec des sujets politiques (pour un aperçu de l'affaire Cambridge Analytica, v. E. Albert, « Cambridge Analytica, la start-up qui influence les électeurs », *Le Monde* 14 avr. 2017).

enregistrés dans une base de données[5]. Cet enregistrement systématique contribue à l'élaboration de portraits de plus en plus précis et détaillés des personnes[6]. Comme le remarquait déjà le doyen Hauriou à propos de la personnalité, « plus la civilisation progresse, plus la personnalité juridique se rapproche de la personnalité réelle ; ce qu'il y a d'excessif dans sa continuité artificielle s'atténue »[7]. L'enregistrement des goûts, hésitations, attirances, déceptions, contribue à atténuer la distinction entre la personne et les données qui la représentent. Nous vivons donc dans une *société de données*, dans laquelle tout mouvement, même trivial ou sans intérêt apparent, est retranscrit et enregistré[8].

Cette société de données inquiète et fait redouter l'avènement d'un monde dans lequel l'homme serait réduit à une suite de chiffres[9].

3. Des espoirs. Dans le même temps, l'informatique a suscité l'espérance d'une société mieux informée, plus prospère et plus libre[10]. Cet espoir s'est notamment matérialisé par le développement de technologies garantissant une protection sans précédent de certains aspects de nos vies privées[11]. Par exemple, si le principe philosophique, moral et juridique de l'inviolabilité des correspondances est posé depuis fort longtemps, son application a toujours trouvé d'importantes limites[12]. Comme le remarquait Voltaire, non sans une pointe d'humour, « jamais le ministère qui a eu le département des Postes n'a ouvert les lettres d'aucun particulier, excepté quand il a eu besoin de savoir ce qu'elles contenaient »[13]. Actuellement, grâce à certaines technologies de chiffrement, notamment le chiffrement de bout en bout[14], une *confidentialité technologique* des échanges d'informations est désormais possible. En

---

[5] D. Cardon, *À quoi rêvent les algorithmes : nos vies à l'heure des big data,* Seuil, 2015, p. 7.
[6] À ce titre, les autoportraits de Cindy Sherman dans lesquels l'artiste se met en scène dans des costumes et des attitudes variés, invitent l'observateur à se questionner sur l'identité et ses modes de représentation.
[7] M. Hauriou, « De la personnalité comme élément de la réalité sociale », *Revue générale du droit* 1898, p. 20.
[8] Sur le besoin de prendre appui sur des choses pour établir des mesures, voir l'analyse d'Alain Desrosières de la règle de méthodologie sociologique de Durkheim selon laquelle « il faut traiter les faits sociaux comme des choses », A. Desrosières, *La politique des grands nombres. Histoire de la raison statistique,* La Découverte, 2010, p. 7 s.
[9] J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 118 s.
[10] P. Kayser, *La protection de la vie privée*, 2e éd., Economica, 1990, no 251, p. 313.
[11] Pour une présentation des effets antagonistes des technologies numériques sur les libertés et notamment sur la protection de la vie privée, v. not. A. Bensamoun, « Les droits fondamentaux et Internet », in *Libertés et droits fondamentaux 2020*, dir. R. Cabrillac, 26e éd., Dalloz, 2020, p. 307 s. ; H. Oberdorff, *Droits de l'homme et libertés fondamentales,* 7e éd., LGDJ, 2019, no 302, p. 411. V. déjà, A. Lucas, J. Devèze et J. Frayssinet, *Droit de l'informatique et de l'Internet*, PUF, 2001, nos 6 s., p. 7 s.
[12] J. Ricard, *Droit et jurisprudence en matière de postes, télégraphes, téléphones*, t. 1, Sirey, 1931, p. 110.
[13] Voltaire, *Dictionnaire philosophique*, t. 20, 1878, p. 257.
[14] A. Greenberg, « Hacker lexicon : what is end-to-end encryption ? », *Wired* 25 nov. 2014.

cas d'interception par un tiers, le déchiffrement de ces communications ne peut aboutir, empêchant *de facto* l'atteinte au secret des correspondances. Dans le domaine des statistiques, c'est la confidentialité différentielle qui offre des promesses nouvelles d'analyses de données respectueuses de la vie privée des personnes concernées[15]. Le bureau américain du recensement a recours à cette technique afin de garantir une meilleure protection des données dans le cadre du recensement décennal de 2020[16]. Les technologies actuelles suscitent donc craintes et espoirs pour ce qui a trait aux libertés individuelles, et particulièrement au droit au respect de la vie privée.

4. La vie privée, une protection juridique récente. Contrairement à une opinion répandue, la protection juridique de la vie privée et de ses différents bastions n'a jamais reçu de garanties aussi amples et diverses que celles qui lui sont reconnues depuis le milieu du XX^{e} siècle[17]. À première vue, on pourrait penser que le besoin de bénéficier d'espaces de solitude ou d'intimité est un sentiment très ancien[18]. En réalité, cette revendication est plutôt récente, et une présentation à grands traits de l'histoire occidentale de la vie privée le prouve[19]. Sous l'Antiquité par exemple, l'État occupait une place telle que la liberté individuelle ne pouvait exister[20]. La personne, réduite au « citoyen », n'était pas autonome par rapport au groupe[21]. Rien dans l'homme n'était indépendant : son corps était au service de l'État et voué à sa défense ; quant à sa fortune, elle appartenait à la Cité qui pouvait en disposer si besoin[22]. Les aspects de sa vie privée n'échappaient pas à cette omnipotence de l'État puisque certaines lois interdisaient même à l'homme de rester célibataire[23].

---

[15] La confidentialité différentielle est un procédé visant à traiter les données pour réduire les risques d'identification des personnes, tout en augmentant la pertinence des résultats fournis, v. C. Dwork, « Differential privacy », in *International Colloquium on Automata, Languages, and Programming*, Springer, 2006, p. 1 s.

[16] J. Abowd, « The U.S. census bureau adopts differential privacy », in *KDD' 18*, Londres, août 2018. Pour une présentation des techniques mises en œuvre, v. US Census Bureau, « Statistical safeguards », 5 août 2020.

[17] Pour un bref exposé de la reconnaissance limitée des protections de l'intimité par le passé, v. J. Antippas et B. Beignier, « La protection de la vie privée », in *Libertés et droits fondamentaux 2020*, R. Cabrillac (dir.), 26^{e} éd., Dalloz, 2020, n^{o} 253, p. 204.

[18] J. Carbonnier, *Droit civil. 1/ Les personnes*, 21^{e} éd., PUF, 2000, n^{o} 96, p. 171.

[19] Bien sûr, il ne s'agit pas d'affirmer que la vie privée n'existait pas avant l'époque moderne, mais plutôt que les dynamiques sociales étaient plus collectives. Pour une étude complète dédiée à l'histoire de la vie privée, v. G. Duby et P. Ariès (dir.), *Histoire de la vie privée*, t. 1 à 5, Seuil, 1999.

[20] F. de Coulanges, *La Cité antique. Étude sur le culte, le droit, les institutions de la Grèce et de Rome,* 1866, Cambridge University Press, réimpr. 2009, p. 281.

[21] J. Mourgeon, *Les droits de l'homme*, 8^{e} éd., PUF, 2008, p. 22.

[22] F. de Coulanges, *La Cité antique. Étude sur le culte, le droit, les institutions de la Grèce et de Rome,* 1866, Cambridge University Press, réimpr. 2009, p. 281 s.

[23] J. S. Mill, *De la liberté*, Gallimard, 1990, p. 80 ; F. de Coulanges, *La Cité antique. Étude sur le culte, le droit, les institutions de la Grèce et de Rome,* 1866, Cambridge University Press, réimpr. 2009, p. 281.

Au Moyen-Âge, l'individu vit en communauté et la séparation entre vie privée et vie publique n'est pas tolérée : celui qui s'isole est souvent soupçonné de complot[24]. D'ailleurs, la densité sociale n'était pas propice à une telle autarcie[25]. C'est pendant la Renaissance que la sphère privée commence à s'esquisser[26]. Le développement de l'imprimerie et de l'alphabétisation dessine un nouvel intérêt pour l'isolement, permettant aux personnes de laisser libre cours à leurs pensées et de développer leur personnalité de manière autonome[27].

La première moitié du XVII[e] siècle marque l'émergence d'un nouveau type de rapport à soi-même et aux autres[28], lequel se caractérise notamment par d'importantes évolutions dans l'architecture du domicile[29]. En raison d'une appétence pour une vie sociale choisie et non plus imposée, l'habitat se divise progressivement entre des espaces de représentation et des espaces privés[30].

Les revendications matérielles se transforment rapidement en revendications sociales et quelques garanties juridiques sont progressivement reconnues dans les démocraties modernes, notamment à l'égard du domicile, des correspondances, et

---

[24] D. Chauvet, *La vie privée. Étude de droit privé,* th. Paris-Sud, 2014, n° 2, p. 3.
[25] P. Ariès, *L'enfant et la vie familiale sous l'Ancien Régime*, Seuil, 1973, p. 299.
[26] En théorisant la place de l'État, Machiavel et Bodin ont notamment contribué à en définir les contours. L'étatisation a ainsi favorisé l'individualisation. Pour Monsieur Jean-Philippe Genet, l'État moderne apparaît comme « le cadre socio-politique indissociable de l'autonomisation de l'individu dans la culture occidentale », J.-P. Genet, « La genèse de l'État moderne. Les enjeux d'un programme de recherche », *Actes de la Recherche en Sciences Sociales* 1997, p. 6. Sur les liens entre l'art, la place de l'État et l'individus, v. C. Le Bart, *L'individualisation*, Presses de Sciences Po, 2008, p. 53 s.
[27] P. Kayser, *La protection de la vie privée par le droit*, 3[e] éd., Economica, 1995, p. 13. La reconnaissance d'une meilleure place de l'individu doit également être mise en perspective avec la religion catholique et les critiques qu'elle reçoit notamment d'Érasme puis Luther ou Calvin. Pour une brève analyse de ces tendances, v. not. J.-M. Baldner, « Sur la naissance de l'individu », *Espace temps* 1988, vol. 37, p. 25 s.
[28] L'émergence progressive de la signature des tableaux est une illustration de ce nouveau type de rapport à soi et aux autres, v. C. Guichard, « La signature dans le tableau aux XVII[e] et XVIII[e] siècles : identité, réputation et marché de l'art », *Sociétés et représentations* 2008, n° 25, p. 47.
[29] Dans un essai, Virginia Wolf rappelait l'importance des espaces personnels pour la création. Ces espaces sont garantis par des aménagements matériels, notamment un verrou sur une porte. « Elle vous a dit comment elle était parvenue à la conclusion – toute prosaïque – qu'il est indispensable d'avoir un revenu de cinq cents livres par an et une pièce munie d'un verrou si vous voulez écrire de la fiction ou de la poésie. » Elle poursuit quelques pages plus loin en affirmant que « La liberté intellectuelle dépend de choses matérielles. La poésie dépend de la liberté intellectuelle. Et les femmes ont toujours été pauvres, pas seulement depuis deux cents ans, mais depuis que le monde est monde. Les femmes ont joui d'une liberté intellectuelle moindre que les fils des esclaves athéniens. Aussi les femmes n'ont pas eu la moindre chance d'écrire de la poésie. C'est pourquoi j'ai tant insisté sur la nécessité d'un revenu et d'une pièce à soi », v. V. Wolf, *A room of one's own,* Feedbooks, 1929, p. 87 s., trad. J.-Y. Cotté. Mais le verrou (symbole de l'intimité) est également le signe d'une porte qui se ferme et qui permet à l'homme d'agir à l'abri des regards, v. par ex. le célèbre tableau de Fragonard *Le Verrou* qui représente, sans doute, « de manière délicate une scène de viol », v. M. Lesauvage, « "Le Verrou" de Fragonard : analyse d'un chef-d'œuvre de l'érotisme », *BeauxArts* 15 sept. 2015. Une partie de la littérature féministe américaine a critiqué la reconnaissance juridique de la vie privée qui cantonnait la femme aux seuls espaces domestiques et qui était invoquée pour empêcher la poursuite d'actes répréhensibles conduits à l'intérieur des foyers, v. not. C. MacKinnon, « Privacy v. Equality : Beyond Roe v. Wade », in *Feminism Unmodified. Discourses on life and law*, dir. C. MacKinnon, Harvard University Press, 1988, p. 93 s. ; A. Allen, *Uneasy access : privacy for women in a free society,* Rowman & Littelfield, 1953.
[30] M. Eleb et A. Debarre, *Architectures de la vie* privée, Hazan, 1999, p. 181.

contre les divulgations par la presse d'éléments de la vie privée[31]. Ces protections étaient relativement fragiles comme l'illustre l'absence de reconnaissance d'une protection transversale de la vie privée par la déclaration des droits de l'homme[32] et le code civil[33].

5. La consécration juridique du droit au respect de la vie privée et de la protection des données à caractère personnel. C'est particulièrement au lendemain de la Seconde Guerre mondiale que le droit s'est imprégné de préoccupations liées à la protection des êtres humains en tant qu'individus uniques[34], ainsi que de l'importance de protéger leur personnalité et leur dignité[35]. Depuis, on ne compte plus les déclarations de droits proclamant la protection des droits de l'homme et notamment le droit au respect de la vie privée[36]. En témoignent particulièrement l'article 12 de la Déclaration universelle des droits de l'homme[37], l'article 17 du Pacte international relatif aux droits civils et politiques[38], l'article 8 de la Convention de sauvegarde des droits de l'homme[39] ou l'article 7 de la Charte des droits fondamentaux de l'Union européenne[40]. La protection des données personnelles a suivi ce mouvement de fondamentalisation puisqu'elles sont désormais protégées par plusieurs sources supranationales telles que la Convention 108 du Conseil de l'Europe[41], les lignes

---

[31] Pour une étude de la reconnaissance de ces protections juridiques, v. D. Chauvet, *La vie privée. Étude de droit privé,* th. Paris-Sud, 2014, n^os^ 2 s., p. 1 s. L'article de doctrine de Louis Warren et Samuel Brandeis publié dans la revue de droit d'Harvard en 1890 a posé les premières pierres de la reconnaissance de la protection de la vie privée, L. Brandeis et S. Warren, « The right to privacy », *Harvard Law Review* 1890, vol. 4, p. 193 s. [4 HARV. L. REV. 193]. Pour une traduction de cet article, v. S. Warren et L. Brandeis, « Le droit à la vie privée », trad. F. Michaud. Cet article a eu un rayonnement international important comme le relève Monsieur Jean-Louis Halpérin, J.-L. Halpérin, « L'essor de la "privacy" et l'usage des concepts juridiques », *Droit et Société* 2005, n^o^ 61, p. 765 s.

[32] En dépit des importants échanges entre les révolutionnaires français et américains, la France ne s'est pas inspirée du Quatrième amendement et n'a pas retenu de protection de la vie privée dans la Déclaration des droits de l'homme et du citoyen. Les correspondances entre Georges Washington et le Marquis de Lafayette sont les témoins de ce dialogue, v. par ex. Lettre de Georges Washington à l'intention du Marquis de Lafayette du 7 février 1788, Mount Vernon. Plus largement, sur l'histoire et la consécration des droits de l'homme, v. L. Favoreu *et al.*, *Droit des libertés fondamentales*, 7^e^ éd., Dalloz, 2015, n^o^ 16, p. 13 s.

[33] Le code civil de 1804 se concentre sur le droit des biens au détriment du droit des personnes : « ce qui domine, c'est l'avoir, bien plus que l'être », F. Terré et D. Fenouillet, *Droit civil. Les personnes*, 8^e^ éd., Dalloz, 2012, n^o^ 1, p. 1. Ce n'est qu'en 1970, avec la loi n^o^ 70-643 du 17 juill. 1970 tendant à renforcer la garantie des droits individuels des citoyens, que l'article 9 du code civil garantissant un droit au respect de la vie privée a été introduit dans le code civil, *JORF* 19 juill. 1970, n^o^ 0166, p. 6755.

[34] G. Goubeaux, *Traité de droit civil. Les personnes*, LGDJ, 1989, n^o^ 271, p. 243 s.

[35] J. Rochfeld, *Les grandes notions du droit privé,* 2^e^ éd., PUF, 2013, *V^o^* « La personne », n^o^ 1, p. 10.

[36] Monsieur Henri Oberdorff emploie même les termes « d'inflation des proclamations », v. H. Oberdorff, *Droits de l'homme et libertés fondamentales,* 7^e^ éd., LGDJ, 2019, n^o^ 16, p. 36.

[37] ONU, Déclaration universelle des Droits de l'Homme, 10 déc. 1948.

[38] ONU, Pacte international relatif aux droits civils et politiques, 16 déc. 1966.

[39] Conseil de l'Europe, Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, 4 nov. 1950.

[40] Charte des droits fondamentaux de l'Union européenne, *JOUE* 30 mars 2010, C-83/02, p. 389 s.

[41] Conseil de l'Europe, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* n^o^ 108, 28 janv. 1981 (dite Convention 108).

directrices de l'OCDE[42], ou l'article 8 de la Charte des droits fondamentaux de l'Union européenne[43].

6. La mise en œuvre légale. Contrairement à l'article 9 du code civil qui pose dans son premier alinéa une maxime générale selon laquelle « chacun a droit au respect de sa vie privée », le droit des données à caractère personnel prévoit un nombre conséquent de règles qu'il est difficile de résumer en quelques mots[44]. Ces règles se répartissent principalement entre la célèbre loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978[45], et le non moins célèbre règlement européen adopté 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 (ci-après « règlement européen »)[46]. Cet intitulé met en lumière un double mouvement de protection des personnes physiques. D'une part, le texte se propose de protéger les personnes à l'égard des traitements de données à caractère personnel[47]. Il ressort de ce premier mouvement que le législateur considère que ces traitements font peser des risques sur la protection des personnes, risques qu'il se propose d'encadrer ou de

---

[42] OCDE, Lignes directrices du 23 sept. 1980 sur la vie privée et les flux transfrontières de données à caractère personnel.

[43] P. de Hert et S. Gutwirth, « Data protection in the case law of Strasbourg and Luxembourg : constitutionalisation in action » et S. Rodotà, « Data protection as a fundamental right », in *Reinventing data protection ?,* dir. S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwangne et S. Nouwt, Springer, 2009, p. 3 s. et p. 77 s. ; G. González Fuster, *The emergence of personal data protection as a fundamental right of the EU*, Springer, 2014 ; E. Debaets, *Le droit à la protection des données à caractère personnel. Recherche sur un droit fondamental*, th. Paris I, 2014, p. 245 ; S. Peyrou, « La protection des données à caractère personnel : un droit désormais constitutionnalisé et garanti par la CJUE », in *La protection des droits fondamentaux dans l'Union européenne*, dir. R. Tinière et C. Vial, Bruylant, 2015, p. 213 s.

[44] « It is impossible to summarise data protection in two or three lines » pouvant être traduit par « il est impossible de résumer la protection des données en deux ou trois lignes », P. de Hert, S. Gutwirth, « Data protection in the case law of Strasbourg and Luxembourg : constitutionalisation in action », in *Reinventing data protection ?,* dir. S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwangne et S. Nouwt, Springer, 2009, p. 3.

[45] Loi nº 78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* 7 janv. 1978, nº 6, p. 227. Depuis son adoption, ce texte a subi d'importantes modifications, particulièrement en 2004 et en 2018, v. loi nº 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi nº 78-17 du 6 janvier 1978, *JORF* du 7 août 2004, nº 0182, p. 14063 ; et loi nº 2018-493 du 20 juin 2018 relative à la protection des données personnelles, *JORF* 21 juin 2018, nº 0141, texte 1. Le Parlement a habilité, par voie d'ordonnance, le Gouvernement à réorganiser cette loi, v. ordonnance nº 2018-1125 du 12 déc. 2018 prise en application de l'article 32 de la loi nº 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, *JORF* 13 déc. 2018, nº 0288, texte 5.

[46] Règlement UE nº 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, *JOUE* 4 mai 2016, L-119/1, p. 1 s. Ce texte a remplacé la directive du même nom adoptée le 24 octobre 1995 et qui a généralisé, à l'échelle communautaire, le droit à la protection des données à caractère personnel, v. directive CE nº 95/46 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, *JOUE* 23 nov. 1995, L-281/31, p. 31 s.

[47] Il est d'ailleurs intéressant de remarquer que le législateur n'a pas souhaité utiliser l'adjectif possessif « leurs » lorsqu'il faisait référence aux données à caractère personnel.

limiter. D'autre part, le texte est relatif à la protection des personnes à l'égard de la libre circulation des données. Ici encore, c'est face à un risque identifié que les règles sont censées apporter des garanties juridiques. Au-delà de cette annonce ambitieuse, il est possible de s'interroger sur la portée véritable de la protection des personnes résultant de ces règles. D'autant que l'intitulé du règlement européen montre que le droit des données à caractère personnel n'est qu'un pan des règles visant la protection des personnes.

7. Plan de l'introduction. Pour cerner les contours de cette étude, il convient dans un premier temps d'en déterminer l'objet (§ I), puis d'évoquer la méthode retenue (§ II).

§ I. Objet de l'étude

8. Droit ou protection des données à caractère personnel ? Il est fréquent de voir le droit des données à caractère personnel présenté sous l'appellation « protection des données à caractère personnel », laissant ainsi présumer que la matière pourrait se résumer à cette protection. Par exemple, lorsque les éditions Dalloz ont publié, en 2018, la première version d'un code dédié à cette matière, ils l'ont dénommé le « code de la protection des données personnelles ». Une telle assimilation entre le droit et la protection qui en découle ne serait-elle pas trompeuse puisque cette matière navigue entre une pluralité d'intérêts[48] ? En effet, le droit des données à caractère personnel est avant tout un droit d'équilibre mettant en balance des intérêts de nature différente, voire contradictoire[49]. Certes, il reconnaît des droits aux personnes concernées et pose un principe de loyauté des traitements de données[50], mais il vise aussi à instaurer un

[48] Selon Monsieur Nicolas Ochoa, « l'expression "protection des données personnelles" constitue souvent un raccourci impropre pour désigner l'ensemble des instruments juridiques encadrant l'activité de traitement de données personnelles. Si l'on prend la peine de se pencher sur l'économie de leurs dispositions, on se rend compte assez rapidement que ces textes sont structurés autour d'un objectif, libéraliser l'activité de traitement de données personnelles – autrement dit ficher les personnes –, et d'une limite, protéger les personnes concernées de l'abus de fichage », N. Ochoa, « La spécificité de la protection des données personnelles en matière fiscale. L'exemple de l'annulation probable du FATCA », *Gestion et Finances Publiques* 2016, nº 6, p. 75.

[49] Pour un rappel de ces intérêts et de leur articulation, v. par ex. Commission, COM2020 66, « Communication de la Commission au Parlement européen et au Conseil, au Comité économique et social européen et au Comité des régions. Une stratégie européenne pour les données », 19 févr. 2020, et Commission, COM2020 264, « Communication de la Commission au Parlement européen et au Conseil. La protection des données : un pilier de l'autonomisation des citoyens et de l'approche de l'Union à l'égard de la transition numérique – deux années d'application du règlement général sur la protection des données », 24 juin 2020.

[50] Pour Madame Olivia Tambou, la protection des données serait plurielle dès lors qu'elle reposerait sur une conciliation entre plusieurs visions. La protection des données devrait d'abord être envisagée comme un droit permettant aux individus de *contrôler* les données les concernant ; ensuite, elle comporterait un certain nombre

marché intérieur européen reposant sur la libre circulation des données[51]. En ne limitant pas son domaine à la protection des données personnelles, la présente étude retient une vision d'ensemble de la matière et de la réalité de ses effets sur la protection des personnes.

9. Le droit des données personnelles, droit transversal. Déterminer le domaine auquel appartient le droit des données à caractère personnel est une opération complexe[52]. Droit *sui generis* ? Droit de la personnalité ? Liberté individuelle ? Certains auteurs rattachent la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés au droit de l'informatique. Son objet est effectivement d'encadrer et de réguler cette matière comme le démontre son article 1er sanctifiant le principe selon lequel « l'informatique doit être au service de chaque citoyen ». Pourtant, selon Jean Carbonnier, cette loi s'inscrit surtout dans les balancements classiques du droit français[53]. D'autant que, même si elle a été conçue et reçue comme une loi de droit public, elle concerne aussi le droit civil et les libertés civiles. Assurément, ce droit transcende la distinction classique opérée par le système juridique français entre droit public et droit privé[54]. L'importance de cette distinction dans la pensée juridique française explique sans doute en partie le faible intérêt porté par la doctrine généraliste à cette matière : faute d'être rattachable à une discipline spécifique, le droit des données à caractère personnel a longtemps été peu étudié. D'ailleurs, les juristes s'en font souvent une image de droit de spécialistes, en rapport avec l'informatique, finalement assez éloigné des questionnements traditionnels. La présente étude s'attachera à montrer que cette matière mobilise la majorité des branches du droit.

---

d'obligations à l'égard des responsables du traitement relatives à la *loyauté* des traitements ; enfin, elle aurait pour objectif d'assurer une gestion des risques au regard des droits et libertés des individus, v. O. Tambou, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, nos 35 s., p. 32 s.

[51] Selon Messieurs Jeremy Antipass et Bernard Beignier, « le RGPD fut adopté pour des raisons principalement économiques tenant à la volonté de permettre l'émergence d'un marché numérique commun entravée par des législations nationales trop disparates (ce que n'avait pas suffi à éviter la directive) », J. Antippas et B. Beignier, « La protection de la vie privée », in *Libertés et droits fondamentaux 2020*, dir. R. Cabrillac, 26e éd., Dalloz, 2020, no 275, p. 233.

[52] Pour Monsieur Alain Supiot, « la division du droit en branches est un produit relativement récent de la dogmatique juridique, puisqu'elle n'a commencé à s'établir qu'au XVIème siècle avec les juristes humanistes de la Renaissance et les théoriciens du droit de la Réforme », A. Supiot, *La gouvernance par les nombres. Cours au Collège de France (2012-2014)*, Fayard, 2015, p. 20.

[53] J. Carbonnier, *Droit civil,* vol. 1, *Introduction. Les personnes. La famille, l'enfant, le couple*, PUF, 2004, no 287, p. 535.

[54] P. Ancel, « La protection des données personnelles : aspects de droit privé français », *RID comp.* 1987, vol. 39, no 3, p. 609, spéc. p. 611.

10. Une approche spécifique du droit des données à caractère personnel. Du fait de l'étendue du droit des données à caractère personnel, un éclairage particulier est nécessaire, au risque sinon de survoler l'ensemble de la matière. Plusieurs thèses de doctorat se sont d'ailleurs déjà intéressées à certains aspects du droit des données à caractère personnel. Des auteurs se sont concentrés sur la notion de donnée personnelle[55], de donnée sensible[56], ou sur la fondamentalisation de ce droit[57]. D'autres auteurs ont tenté de démontrer que l'objectif principal de la matière n'était pas la protection des personnes fichées, mais plutôt la liberté des traitements[58] ; d'autres encore ont étudié le besoin d'adaptation de ce droit aux développements technologiques[59]. Ces études n'épuisent en rien le sujet des données à caractère personnel. Au contraire, elles illustrent la variété des enjeux soulevés par cette matière et le besoin d'analyses de fond. Notre étude s'inscrit dans ces travaux et retient un nouvel éclairage d'analyse de ce droit. Le choix de cet éclairage s'est fondé sur une incompréhension résultant du décalage entre la *protection des personnes* telle qu'elle est annoncée, recherchée ou ressentie par les individus, et celle qui existe en réalité. Cette dissonance entre des règles juridiques perçues comme garantissant une protection des personnes d'une part et la substance concrète de ces règles ainsi que leur mise en œuvre d'autre part, nous a encouragée à analyser la substance de la protection des personnes résultant du droit des données à caractère personnel. Pour cela, encore faut-il s'entendre sur ce que recouvre la notion de protection des personnes.

11. La protection des personnes. Si l'expression « protection des personnes » est familière aux juristes, il est difficile d'en trouver une définition faisant l'unanimité[60].

---

[55] F. Lesaulnier, *L'information nominative,* th. Paris II, 2005 ; P.-Y. Marot, *Les données et informations à caractère personnel. Essai sur la notion et ses fonctions,* th. Nancy, 2007 ; J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon ; S. Alliot, *Essai de qualification de la notion de données à caractère personnel,* th. Besançon, 2018.

[56] R. Brasselet, *La circulation de la donnée à caractère personnel relative à la santé*, th. Lorraine, 2018 ; C. Koumpli, *Les données personnelles sensibles. Contribution à l'évolution du droit fondamental à la protection des données à caractère personnel*, th. Paris I, 2019.

[57] E. Debaets, *Le droit à la protection des données à caractère personnel. Recherche sur un droit fondamental*, th. Paris I, 2014 ; N. Chambardon, *L'identité numérique de la personne humaine : contribution à l'étude du droit fondamental à la protection des données à caractères personnel,* th. Lyon II, 2018.

[58] N. Ochoa, *Le droit des données personnelles, une police administrative spéciale*, th. Paris I, 2014.

[59] J. Le Clainche, *L'adaptation du droit des données à caractère personnel aux communications électroniques,* th. Montpellier I, 2008 ; É. Gratton, *Redefining personal information in the context of the Internet*, th. Paris II et Montréal, 2012 ; M. Lanna, *La protection des données à caractère personnel à l'épreuve de l'automesure connectée*, th. Paris II, 2019. V. aussi, dans le domaine de la recherche, I. Coulibaly, *La protection des données à caractère personnel dans le domaine de la recherche scientifique*, th. Grenoble, 2011.

[60] Dans sa thèse pourtant dédiée à la protection des personnes contre la réalisation et la publication de leur image, Monsieur Jacques Ravanas ne s'aventurait pas à proposer une définition de cette notion, J. Ravanas, *La protection des personnes contre la réalisation et la publication de leur image*, th. Aix-en-Provence, 1978, LGDJ.

Longtemps, l'expression était assimilée aux mesures de protection juridique prévues pour aider une personne vulnérable à protéger ses intérêts[61]. D'ailleurs, le Vocabulaire juridique de l'Association Henri Capitant définit la protection comme la « précaution qui, répondant au besoin de celui ou de ce qu'elle couvre et correspondant en général à un devoir pour celui qui l'assure, consiste à prémunir une personne ou un bien contre un risque, à garantir sa sécurité, son intégrité, etc., par des moyens juridiques ou matériels »[62]. Aujourd'hui, cette expression s'entend plus largement, et le droit protège la personne d'une double manière[63]. De façon générale, la protection des personnes est assurée par le respect des libertés individuelles et des droits de la personnalité[64]. De façon spécifique, la loi organise la protection de certaines personnes, en raison de leur vulnérabilité. L'expression « protection des personnes » s'est donc libérée de sa conception initialement restrictive et s'entend désormais largement[65].

12. L'angle de la protection des personnes. Le choix de l'expression « protection des personnes » dans le cadre d'une étude dédiée au droit des données à caractère personnel paraît doublement justifié. D'une part, en matière de données à caractère personnel, il est fréquent que la personne concernée se trouve dans un état d'ignorance, ou au moins de méconnaissance, des traitements effectués sur ses données[66]. Le droit intervient alors pour prémunir la personne concernée contre un risque lié aux traitements de ses données ; il lui apporte garanties et protections[67]. D'autre part, cette expression rappelle la variété des intérêts pris en compte par le droit des données à caractère personnel. En effet, celui-ci n'a pas pour seul objectif de protéger les personnes dès lors que sa fonction complémentaire est d'organiser les conditions de licéité des traitements de données personnelles et leur circulation dans l'espace européen. Surtout, ce droit a vocation à s'articuler avec d'autres droits et libertés dans

---

[61] V. par ex. B. Teyssié, *Droit des personnes*, 21e éd., LexisNexis, 2019, no 653, p. 435 s.
[62] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vo* « Protection », sens 1.
[63] A. Marais, *Droits des personnes*, 3e éd., Dalloz, 2018, no 232, p. 157 ; B. Beignier et J.-R. Binet, *Droit des personnes et de la famille*, 4e éd., LGDJ, 2019, no 332, p. 223.
[64] J. Carbonnier, *Droit civil,* vol. 1, *Introduction. Les personnes. La famille, l'enfant, le couple*, PUF, 2004, nos 274 s., p. 510 s.
[65] Monsieur Grégoire Loiseau relève que « le respect de la personne humaine est une préoccupation relativement récente du droit. (…) À cet égard, la reconnaissance de droits investissant chaque personne de façon égale, du seul fait de son humanité, correspond au passage d'une protection désincarnée de l'individu, assurée au moyen de règles de droit objectif – responsabilité civile, normes pénales –, à la consécration de droits subjectifs permettant à chacun d'être en mesure de faire valoir sa propre protection », G. Loiseau, *Le droit des personnes*, 2e éd., Ellipses, 2020, no 211, p. 169.
[66] Sur l'idée que la donnée personnelle est une information hors du contrôle de l'individu, v. J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 141.
[67] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vo* « Protection », sens 1.

lesquelles la protection des personnes trouve également toute sa place[68]. Comment nier l'importance des libertés individuelles, notamment la liberté d'expression ou d'information, dans la protection des personnes ? Face à cette pluralité d'objectifs pris en compte par ce droit, le recours à la notion de protection des personnes s'est révélé précieux.

13. Protection des personnes ou de la personne concernée ? Le choix du pluriel dans l'expression « protection des personnes » se fonde sur le souci de mettre en exergue le fait que le droit des données à caractère personnel ne se limite pas à la protection de l'intérêt de la personne concernée par les traitements de ses données. La matière s'étend aussi, certes dans une moindre mesure, aux intérêts de la société dans son ensemble. Cette conception large du champ de protection couvert par la loi se retrouve notamment dans la formule coiffant la loi du 6 janvier 1978 selon laquelle l'informatique « 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 »[69]. Elle se retrouve également dans l'intitulé du Règlement européen qui se propose de protéger les personnes physiques à l'égard des traitements de données à caractère personnel et non pas seulement des traitements de « leurs » données à caractère personnel. En ressort ainsi une vision collective des risques liés aux traitements de données à caractère personnel. Les risques liés à ces traitements ne se limiteraient pas seulement à la personne concernée, mais s'étendraient à l'ensemble de la société. Ainsi, ce sont également les libertés des autres personnes qui seront étudiées, notamment leur liberté d'information, d'expression ou leur autonomie personnelle. Pour autant, notre étude se limitera à l'étude de la protection des personnes physiques et ne s'étendra pas à celle des personnes morales. Un tel choix se justifie aisément : ce sont les personnes physiques qui sont les sujets visés par ces règles, et les personnes morales n'y trouvent qu'une place indirecte[70].

---

[68] Le considérant 4https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR - d1e2097-1-1 du règlement UE n° 2016/679 prévoit d'ailleurs que « le droit à la protection des données à caractère personnel n'est pas un droit absolu ; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité ».

[69] Pour une analyse de cette formule et des libertés protégées par la loi Informatique et libertés, A. Lucas, J. Devèze et J. Frayssinet, *Droit de l'informatique et de l'Internet*, PUF, 2001, n^os^ 34 s., spéc. p. 21 s.

[70] On doit tout de même remarquer que les personnes morales tentent souvent de bénéficier des protections prévues par le droit des données à caractère personnel, v. *infra*, n^os^ 103 s.

14. Conception retenue de la protection des personnes. Pour éviter de manquer des aspects importants des effets du droit des données à caractère personnel, le présent travail retient une conception large de la « protection des personnes », entendue sous l'angle de la *liberté individuelle*. Celle-ci est classiquement définie comme la reconnaissance pour chaque personne d'un espace d'autodétermination lui permettant de faire ses propres choix en termes de déplacement, de domicile ou de vie privée, sans intervention d'une autre personne ou d'une autorité publique[71]. Retenir une telle conception de la protection des personnes était justifié du fait de la particularité des atteintes permises par les traitements de données à caractère personnel s'immisçant de plus en plus amplement dans la liberté d'autodétermination[72]. Près d'un demi-siècle après la publication du Rapport Tricot, le constat énoncé dans ses premières lignes se vérifie toujours : les atteintes aux libertés restent difficiles à démontrer, et leur caractère insidieux s'est renforcé. Sous couvert de bienveillance, les responsables du traitement utilisent aujourd'hui les données à caractère personnel pour de nombreuses finalités, notamment de manipulation.

15. Risques de manipulation des personnes. La publicité ciblée est sans doute le versant le plus connu de la manipulation effectuée par les traitements de données personnelles[73]. Au mieux, le caractère grossier de la publicité excède le voyageur qui vient d'acheter un billet d'avion et qui se voit proposer une location de voiture au meilleur prix. Au pire, cette publicité façonne insidieusement ses intérêts. Publicité après publicité, vidéo après vidéo, article après article, la personne est influencée et manipulée, pour que ses goûts servent des intérêts extérieurs. D'autres domaines, beaucoup plus intimes que ceux liés à notre consommation, sont également soumis à ces algorithmes de recommandation[74]. Par exemple, sous le slogan tapageur « Matchez. Discutez. Faites des rencontres », l'application de rencontres en ligne Tinder fait défiler des profils d'utilisateurs pour faciliter les rencontres. L'utilisateur est invité à

---

[71] H. Oberdorff, *Droits de l'homme et libertés fondamentales,* 7e éd., LGDJ, 2019, no 242, p. 313. L'acception de la liberté individuelle que nous retenons ne se limite donc pas à la conception stricte désormais retenue par le Conseil constitutionnel. Pour une évolution de l'interprétation de cette notion par le Conseil constitutionnel, v. L. Favoreu *et al.*, *Droit des libertés fondamentales*, 7e éd., Dalloz, 2015, nos 218, p. 179 s.

[72] V. *infra*, no 393.

[73] V. parmi de nombreux travaux de sociologie sur cette question, H. Le Crosnier, « Usage des traces par la publicité comportementale », in *Traces numériques. De la production à l'interprétation,* dir. B. Galinon-Melenec et S. Zlitni, CNRS, 2013, p. 91 s., spéc. p. 95.

[74] Le terme algorithme vient de l'arabe, *al-Kharezmi*, surnom d'un savant arabe du IXe siècle, et signifie « ensemble de règles dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations », v. Dictionnaire Larousse, *Dictionnaire de français, Vo* « Algorithme ».

balayer l'écran vers la droite (pour indiquer qu'il apprécie la personne qui lui est présentée) ou vers la gauche (pour signifier que la personne ne lui plaît pas). Derrière ces simples propositions se cachent des traitements complexes. L'un d'entre eux vise à déterminer quelles personnes montrer à l'utilisateur en se fondant sur la prédiction de points communs établis grâce à l'analyse des photographies, des présentations et de toutes les données partagées sur l'application. C'est surtout certains algorithmes, notamment ceux liés au score de désirabilité[75], qui influencent les personnes que nous rencontrons et nous enferment dans un certain déterminisme algorithmique[76]. Mais ces considérations s'appliquent bien plus largement : notre façon de nous informer, nos possibilités d'emprunt, nos opinions, nos repas sont aujourd'hui façonnés par ces algorithmes[77]. Face à ces risques, le droit des données à caractère personnel suffit-il à garantir une protection effective des personnes ? Cette interrogation nous a donc amenée à questionner l'effectivité de la protection des personnes résultant du droit des données à caractère personnel.

16. L'effectivité : un concept fuyant. Si la notion d'effectivité est souvent utilisée par la doctrine, elle n'en est pas moins fuyante[78]. Son étymologie peut toutefois être retracée aisément : l'effectivité est le caractère de ce qui est effectif[79]. Or, l'adjectif effectif est emprunté au latin *effectivus* et signifie « qui produit ; pratique », puis en bas latin, chez les grammairiens, il renvoie à « ce qui exprime un effet »[80]. La définition moderne du terme effectif reprend cette polysémie[81]. Par conséquent, l'effectivité

---

[75] Cette note de désirabilité était élaborée par le traitement et l'analyse de l'activité de l'utilisateur et de celle des autres à son égard (notamment le nombre d'utilisateurs ayant balayé l'écran vers la droite, indiquant qu'ils appréciaient la personne). Après une étude journalistique de Madame Judith Duportail, Tinder a affirmé avoir mis fin à cette note, v. J. Duportail, *L'amour sous algorithme*, Goutte d'or, 2018.

[76] Monsieur Eli Pariser a théorisé le concept de « filter bubble » (bulle de filtres en français), lequel signifie que les traitements d'informations filtrent les informations auxquelles les personnes sont exposées et les enferment dans une sorte de bulle dans laquelle seules certaines informations peuvent entrer, v. E. Pariser, *The filter bubble,* Penguin Press, 2011, p. 6.

[77] P. de Filippi, « Gouvernance algorithmique : vie privée et autonomie individuelle à l'ère des *Big Data* », in *Open data & data protection : nouveaux défis pour la vie privée*, dir. D. Bourcier et P. de Filippi, Mare & Martin, 2016.

[78] J. Betaille, *Les conditions juridiques de l'effectivité de la norme en droit public interne : illustrations en droit de l'urbanisme et en droit de l'environnement,* th. Limoges, 2012, nº 14, p. 14. Dans le domaine de la théorie du droit, Henri Batiffol ne manquait pas de souligner les ambiguïtés de la notion d'effectivité, H. Batiffol, *Problèmes de base de philosophie du droit*, LGDJ, 1979, p. 117 s. ; Monsieur François Rangeon constatait « qu'il ne règne aucun accord sur la signification précise, la portée et le statut de cette notion », F. Rangeon, « Réflexions sur l'effectivité du droit », in *Les usages sociaux du droit*, dir. D. Lochak, PUF, 1989, p. 126.

[79] Larousse, *Dictionnaire de Français, V°* « Effectivité » ; É. Littré, *Le nouveau Littré. Le dictionnaire de référence de la langue française*, Garnier, 2007, *V°* « Effectivité ».

[80] *Dictionnaire de l'Académie française*, 9e éd., *Vº* « Effectif », sens I.

[81] Le terme fait aussi bien référence à « ce qui produit un effet réel », qu'à « ce qui existe réellement », v. *Dictionnaire de l'Académie française*, 9e éd., *Vº* « Effectif », sens I.1 et I.2.

exprime non seulement l'idée selon laquelle quelque chose a produit un effet, mais aussi que quelque chose est réel[82].

Hormis en droit international public où l'effectivité est classiquement invoquée pour justifier la reconnaissance ou l'opposabilité d'une situation ou d'un fait réellement établi[83], l'effectivité a longtemps été étrangère au langage juridique[84]. Le terme s'est émancipé de la conception du droit international public[85], surtout à partir de la seconde moitié du XX^e^ siècle, notamment grâce à l'esprit et la plume de Jean Carbonnier qui y a consacré un article fondateur[86]. Le doyen Carbonnier estimait que « l'effectivité n'est pas ce bloc sur lequel juristes et sociologues se sont trop facilement accordés – pour mieux faire éclater ensuite leur désaccord. C'est une notion toute relative »[87].

17. Multiplicité des approches désignées par l'expression. En droit, l'effectivité est souvent assimilée à l'application de la norme juridique, là où l'ineffectivité renvoie à l'idée de son absence d'application par les autorités chargées de son contrôle[88]. L'analyse de l'effectivité d'une norme revient donc à apprécier son taux d'observation[89]. Certains auteurs critiquent toutefois cette conception en considérant que l'effectivité ne saurait être réduite à la seule réalisation des effets voulus par le législateur ou à l'application des règles énoncées. En effet, ces règles sont susceptibles d'être interprétées de diverses manières[90]. Pour Jean Carbonnier par exemple,

---

[82] J. Betaille, *Les conditions juridiques de l'effectivité de la norme en droit public interne : illustrations en droit de l'urbanisme et en droit de l'environnement,* th. Limoges, 2012, n° 14, p. 14.
[83] S. Guinchard et T. Debard (dir.), *Lexique des termes juridiques*, Dalloz, 2020, *V°* « Effectivité », droit international public. Pour une étude de ce principe en droit international public, v. F. Couveinhes, *L'effectivité en droit international public*, th. Paris II, 2011. Pour une présentation historique de l'effectivité et de la place que ce terme occupe en droit international, v. M. Chemillier-Gendreau, « À propos de l'effectivité en droit international », *Revue belge de droit international* 1975, vol. 11, p. 38.
[84] Selon certains auteurs, ce type d'études ne relèveraient pas de la compétence des juristes. Ainsi, pour Noberto Bobbio, il revient aux juristes de s'intéresser à la validité des règles alors que les sociologues et historiens auraient à se concentrer sur l'effectivité du droit. En effet, selon cet auteur, « la validité est une question qui relève de la théorie générale du droit, la recherche sur l'efficacité ou l'inefficacité d'une norme est une recherche historico-sociologique », N. Bobbio, *Teoria generale del diritto*, Giappichelli, 1993, p. 25. Pour une présentation du façonnage de la notion juridique d'effectivité, v. F. Couveinhes, *L'effectivité en droit international public*, th. Paris II, 2011, p. 32 s.
[85] J. Betaille, *Les conditions juridiques de l'effectivité de la norme en droit public interne : illustrations en droit de l'urbanisme et en droit de l'environnement,* th. Limoges, 2012, n° 5, p. 4.
[86] J. Carbonnier, « Effectivité et ineffectivité de la règle de droit », *L'année sociologique* 1957-1958, vol. 9, p. 3.
[87] J. Carbonnier, « Effectivité et ineffectivité de la règle de droit », *L'année sociologique* 1957-1958, vol. 9, p. 3, spéc. p. 15.
[88] Cela renvoie notamment à la conception de Hans Kelsen, pour qui « un ordre normatif est efficace quand, d'une manière générale, les individus auxquels il s'adresse se conforment à ses normes », H. Kelsen, *La théorie pure du droit. Introduction à la science du droit*, La Braconnière, 1953, p. 25. Sur cette interprétation, v. not. M.-A. Cohendet, « Légitimité, effectivité et validité », in *Mélanges P. Avril,* Montchrestien, 2001, p. 201 s., spéc. p. 203 et p. 218.
[89] C. Tzutzuiano, *L'effectivité de la sanction pénale*, th. Toulon, 2015, n° 9, p. 14.
[90] F. Rangeon, « Réflexions sur l'effectivité du droit », in *Les usages sociaux du droit,* dir. D. Lochak, PUF, 1989, p. 133, spéc. p. 137.

l'effectivité ne se limite pas à une opposition frontale entre ce qui est effectif et ce qui ne l'est pas, mais doit plutôt être appréciée selon différents degrés[91]. Cette idée constitue la richesse essentielle du concept d'effectivité par rapport à d'autres notions connexes telles que celles de mise en œuvre, d'exécution, de respect ou d'efficacité[92].

18. Une étude du droit des données à caractère personnel conduite à la lumière de son effectivité pour la protection des personnes. Contrairement à d'autres études dédiées à l'effectivité[93], le présent travail ne vise pas à sonder l'effectivité d'une règle de droit. Il s'intéresse davantage à l'effectivité d'une matière (le droit des données à caractère personnel) par rapport à un objectif (la protection des personnes). C'est donc en retenant la double acception de l'effectivité que le sujet sera ici étudié, c'est-à-dire non seulement en s'intéressant à l'*effet produit* par le droit des données à caractère personnel sur la protection des personnes, mais aussi en analysant la *réalité de cet effet*.

Une telle interprétation de l'effectivité rejoint celle fournie par les dictionnaires juridiques qui la définissent comme « le caractère réel et concret d'un droit, au-delà de sa reconnaissance abstraite dans des textes de loi »[94]. Cette définition se rapproche également de celle développée par la Cour européenne des droits de l'homme qui affirme régulièrement, depuis son arrêt *Airey*, que « la Convention a pour but de protéger des droits non pas théoriques ou illusoires, mais concrets et effectifs »[95]. La Cour a ainsi utilisé le caractère effectif des droits énoncés par la Convention pour lutter

---

[91] J. Carbonnier, « Effectivité et ineffectivité de la règle de droit », *L'année sociologique* 1957-1958, vol. 9, p. 3, spéc. p. 14.

[92] La notion entretient d'importants rapports avec des notions voisines, notamment d'efficacité ou d'efficience, v. not. P. Conte, « "Effectivité", "inefficacité", "sous-effectivité", "surefficacité"… : variations pour droit pénal », in *Mélanges P. Catala,* Litec, 2001, p. 125 s. M.-A. Frison-Roche, « L'efficacité des décisions en matière de concurrence : notions, critères, typologie », *LPA* 28 déc. 2000, nº 259, p. 4, § 5 s. ; B. Delzangles, « Effectivité, efficacité et efficience dans la jurisprudence de la Cour européenne des droits de l'homme », in *À la recherche de l'effectivité des droits de l'homme*, dir. V. Champeil-Desplats et D. Lochak, Presses Universitaires de Paris Ouest, 2008, p. 41. J. Betaille, *Les conditions juridiques de l'effectivité de la norme en droit public interne : illustrations en droit de l'urbanisme et en droit de l'environnement,* th. Limoges, 2012, nº 15, p. 15.

[93] Souvent, la question de l'effectivité est étudiée par les juristes sous l'angle d'une règle particulière, d'un domaine juridique ou d'une décision, v. par ex. J. Betaille, *Les conditions juridiques de l'effectivité de la norme en droit public interne : illustrations en droit de l'urbanisme et en droit de l'environnement,* th. Limoges, 2012 ; B. Iosca, *L'effectivité de la sanction des infractions au code de la route,* th. Toulon, 2014 ; C. Tzutzuiano, *L'effectivité de la sanction pénale*, th. Toulon, 2015 ; S. Benzina, *L'effectivité des décisions QPC du Conseil constitutionnel*, th. Paris II, 2016, LGDJ.

[94] S. Guinchard et T. Debard (dir.), *Lexique des termes juridiques*, Dalloz, 2020, *Vº* « Effectivité », droit civil. De manière similaire, le Vocabulaire juridique de l'Association Henri Capitant définit l'effectivité comme le « caractère d'une règle de droit qui produit l'effet voulu, qui est appliquée réellement », G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vº* « Effectivité », sens 1.

[95] CEDH, 9 oct. 1979, *Airey* c. *Royaume-Uni*, n° 6289/73, § 24. Plus récemment v. not. CEDH, 1 avr. 2010, *S.H. et autres* c. *Autriche*, n° 57813/00, § 92 s. ; CEDH, 19 juill. 2016, *Călin et autres* c. *Roumanie*, n° 25057/11, nº 34739/11 et nº 20316/12, § 101.

contre la passivité des États et les pousser à adopter des mesures de mise en œuvre[96]. Sans surprise, c'est également cette conception de l'effectivité qui est souvent retenue par les études consacrées aux droits de l'homme[97] ou aux droits des données à caractère personnel[98].

19. Une étude circonscrite géographiquement. À première vue, l'angle de l'effectivité de la protection des personnes pourrait laisser penser que le présent travail va porter sur des questions d'application territoriale du droit des données à caractère personnel. Une acception large de ce sujet pourrait justifier une telle approche. Il est vrai que l'enjeu d'effectivité paraît accru lorsque les données collectées au sein de l'Union européenne par des entreprises étrangères sont transférées vers des serveurs de données situés dans des pays tiers[99].

20. L'application territoriale étendue du droit européen des données à caractère personnel. Pour éviter d'éventuelles stratégies de contournement, le législateur européen a défini largement le champ d'application territorial du règlement européen[100]. Son article 3 pose ainsi trois critères de rattachement. Le premier est un critère d'établissement visant les responsables du traitement ou les sous-traitants établis dans l'Union européenne ; le deuxième est un critère de ciblage visant les responsables du traitement ciblant une personne concernée située sur le territoire européen ; enfin, le troisième critère permet l'application du règlement lorsque le droit d'un État membre s'applique en vertu du droit international public[101]. Ces trois critères

---

[96] B. Delzangles, « Effectivité, efficacité et efficience dans la jurisprudence de la Cour européenne des droits de l'homme », in *À la recherche de l'effectivité des droits de l'homme*, dir. V. Champeil-Desplats et D. Lochak, Presses Universitaires de Paris Ouest, 2008, p. 41, n° 2.
[97] V. par ex. V. Champeil-Desplats, « Effectivité et droits de l'homme : l'approche théorique », in *À la recherche de l'effectivité des droits de l'homme*, dir. V. Champeil-Desplats et D. Lochak, Presses Universitaires de Paris Ouest, 2008, p. 11, n° 3 s.
[98] J.-F. Perrin, « La notion d'"effectivité" en droit européen, international et comparé de la protection des données personnelles », in *Mélanges B. Dutoit,* Librairie Droz, 2002, p. 197 s., spéc. p. 208.
[99] D'ailleurs le règlement UE n° 2016/679 ne manque pas de faire référence au besoin d'effectivité des droits des personnes concernées, notamment à l'occasion des transferts de données (cons. 104 du texte) et du droit à un recours effectif (art. 78 et 79 du texte).
[100] O. Tambou, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, n^os^ 103 s., p. 94 s.
[101] CEPD, Lignes directrices 3/2018 relatives au champ d'application territorial du RGPD (article 3), 12 nov. 2019, p. 4.

garantissent une application particulièrement étendue de ces règles[102]. Certains auteurs parlent même « d'extraterritorialité » de ce texte[103].

À ces principes s'ajoute également une compétence étendue du juge dans cette matière, et ce depuis plusieurs années déjà[104]. D'ailleurs, le règlement a conforté cette compétence étendue du juge national en affirmant dans le second paragraphe de son article 79 que « toute action contre un responsable du traitement ou un sous-traitant est intentée devant les juridictions de l'État membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement. Une telle action peut aussi être intentée devant les juridictions de l'État membre dans lequel la personne concernée a sa résidence habituelle ». Ainsi, le législateur européen reconnaît une option de compétence et se révèle donc assez protecteur de la victime[105]. La compétence du juge français pour les affaires impliquant des victimes ayant leur résidence habituelle en France est donc expressément reconnue. Pour autant, il est vrai que les transferts de données vers des pays tiers posent des difficultés pratiques.

21. Les principes applicables aux transferts de données. En principe, de tels transferts ne sont permis que si le niveau de protection des personnes physiques garanti par le droit européen des données personnelles n'est pas compromis dans ces pays[106]. Le règlement européen prévoit ainsi la licéité des transferts lorsqu'ils sont fondés sur une décision d'adéquation ou, à défaut, lorsque des garanties appropriées sont prévues[107]. Pour les fondements liés aux garanties appropriées, le pouvoir d'appréciation du niveau de protection revient à la Commission, aux autorités de

---

[102] L'articulation de cet article avec les règles issues de la loi française, particulièrement son article 3, n'est pas parfaitement claire, N. Martial-Braz et J. Rochfeld (dir.), *Droit des données personnelles. Les spécificités du droit français au regard du RGPD,* Dalloz, 2019, n^os^ 220 s., p. 44 s.

[103] A. Deroudille et F. Fatah, « L'extraterritorialité du RGPD dans le contexte du "*Cloud Act*" », *RUE* 2019, p. 442 ; P. Jacob, « La compétence des États à l'égard des données numériques : du nuage au brouillard… en attendant l'éclaircie ? », *Revue critique de droit international privé* 2019, p. 665.

[104] Sur la reconnaissance de la compétence du juge français à l'égard de Facebook, v. CA Paris, 2^e^ ch., 12 févr. 2016, n^o^ 15/08624. Plus largement, sur la compétence du juge français en matière de litiges liés à Internet, v. Cour de cassation, « Le juge et la mondialisation dans la jurisprudence de la Cour de cassation », *Étude Annuelle 2017*, La Documentation française, 2017, p. 191 s. À l'inverse, la compétence d'une autorité nationale de contrôle est plus encadrée du fait du mécanisme d'autorité chef de file instauré par l'article 56 du règlement UE n^o^ 2016/679. Pour autant, la question de savoir si l'autorité chef de file a une compétence exclusive vient d'être posée à la Cour de justice de l'Union européenne dans l'affaire C-645/19 opposant l'autorité belge de protection des données à Facebook, F. Yun Chee, « Facebook, Belgian watchdog face off over who should police company », *Reuters* 5 oct. 2020.

[105] F. Jault-Seseke et C. Zolynski, « Le Règlement 2016/679/UE relatif aux données personnelles. Aspects de droit international privé », *D.* 2016, p. 1874.

[106] Art. 44 du règlement UE n^o^ 2016/679.

[107] Pour un exposé relatif aux possibilités de transférer des données en-dehors du territoire européen, v. R. Perray, « Quelle stratégie pour les transferts de données personnelles hors de l'Union européenne à l'aune du RGPD », *CCE* 2018, n^o^ 4, dossier 16.

protection ou à ces deux instances[108] ; quant à la décision d'adéquation, ce pouvoir revient à la Commission européenne[109], sous le vigilant contrôle de la CJUE. À ce titre, dans les affaires *Schrems*, la Cour de justice de l'Union européenne a invalidé les décisions d'adéquation dans lesquelles la Commission européenne constatait que les États-Unis d'Amérique offraient un niveau adéquat de protection[110]. Ces décisions ont engendré d'importantes incertitudes sur la licéité des transferts de données à caractère personnel. Surtout, elles montrent la fragilité de tels instruments et les effets des évolutions juridiques (ou justement leur défaut d'évolution) sur les décisions d'adéquation. Pour autant, l'analyse de ces décisions appellerait d'importants développements analytiques des droits étrangers, notamment des dispositions relatives aux données personnelles et aux programmes de surveillance mis en place dans ces pays[111]. Or de tels développements, bien qu'ils présentent un intérêt incontestable, ne contribuent pas à dégager des tendances générales sur le droit positif tel que mis en œuvre en Europe. D'autant qu'avant de pouvoir mesurer l'effectivité d'un système étranger par rapport au système européen, il faut préalablement déterminer l'effectivité du système européen. Cette détermination appelle d'ores et déjà d'importants développements expliquant cette circonscription géographique. Dans cet objectif, l'éclairage de la protection des personnes est particulièrement utile. Celle-ci commande d'adopter une approche en deux temps.

22. Perspectives de l'étude. Les perspectives de l'étude sont doubles. Tout d'abord, il faut s'assurer que le domaine d'application matériel couvre l'ensemble des données méritant une protection, sans pour autant s'appliquer au-delà de ce qui est

---

[108] Pour un exposé sommaire des modalités de circulation des flux de données, v. not. *Rép. int.* Dalloz, *V°* « Informatique », par M. Vivant et N. Mallet-Poujol, 2019, n^os^ 14 s. ; *Rép. eur.* Dalloz, *V°* « La protection des données personnelles dans les relations internes à l'Union européenne », par C. Castets-Renard, 2018 (actu. 2020), n^os^ 161 s. Pour une analyse pratique de ces règles, v. F. Naftalski, « L'impact du nouveau règlement sur les stratégies de transferts internationaux de données personnelles », *Dalloz IP/IT* 2016, p. 340.

[109] Art. 45 du règlement UE n° 2016/679.

[110] CJUE, 6 oct. 2015, *Maximillian Schrems* c. *Data Protection Commissioner,* C-362/14, § 88 s., et CJUE, 16 juill. 2020, *Data Protection Commissioner* c. *Facebook Ireland Ltd, Maximillian Schrems,* C-311/18, § 168 s. Parmi les nombreux commentaires de la première décision, v. not. C. Castets-Renard, « Invalidation du *Safe Harbor* par la CJUE : tempête sur la protection des données personnelles aux États-Unis », *D.* 2016, p. 88 ; B. Haftel, « Transferts transatlantiques de données personnelles : la Cour de justice invalide le *Safe Harbour* et consacre un principe de défiance mutuelle », *D.* 2016, p. 111 ; C. Thérard-Jallu, K.-M. Job et S. Mintz, « Invalidation de l'accord *Safe Harbor* par la CJUE : portée, impacts et premiers éléments de solution », *Dalloz IP/IT* 2016, p. 26. Parmi les commentaires de la seconde décision, v. not. F. Mattatia, « Données personnelles : la CJUE invalide le Privacy Shield », *JCP A* 2020, n° 36, act. 491 ; T. Douville, « Invalidation du *Privacy Shield* et insuffisance des clauses-types : fin (temporaire ?) des transferts de données à caractère personnel vers les États-Unis », *AJ Contrat* 2020, p. 436.

[111] Dans sa décision du 16 juillet 2020, la CJUE a longuement discuté de ces pratiques de surveillance, CJUE, 16 juill. 2020, *Data Protection Commissioner* c. *Facebook Ireland Ltd, Maximillian Schrems,* C-311/18, § 178 s.

requis. À ce titre, il convient de questionner l'étendue de la notion de donnée à caractère personnel afin de s'assurer qu'elle s'applique aussi strictement que possible mais aussi largement que nécessaire[112]. Cette approche invite ensuite à sonder l'effectivité du régime associé pour vérifier l'adéquation de ces principes aux impératifs de protection. Les principes servent-ils toujours la protection des personnes ou se concentrent-ils sur des intérêts particuliers au détriment de l'intérêt général ?

23. La notion de donnée à caractère personnel, clé de voûte du droit des données personnelles. Au cœur du droit des données personnelles se trouve indiscutablement la notion de donnée à caractère personnel, laquelle est la porte d'entrée conditionnant l'application de son régime[113]. L'étude de cette notion est donc essentielle puisqu'elle circonscrit le domaine matériel de la matière. S'interroger sur l'étendue de la notion est d'autant plus important que celle-ci imprègne notre quotidien.

24. Évolution de la notion. Depuis l'adoption des premières règles du droit des données à caractère personnel, les auteurs s'accordent sur un paramètre élémentaire : la notion de donnée personnelle *doit* être interprétée largement[114]. L'abandon de la notion d'information nominative illustre particulièrement ce mouvement. Considérée comme trop restrictive pour s'adapter aux développements technologiques et intégrer dans son giron l'ensemble des informations indirectement identifiantes, cette notion a été remplacée par celle de donnée à caractère personnel[115].

25. Définition de la notion de donnée à caractère personnel. La définition légale a l'avantage de la simplicité. La donnée à caractère personnel est « toute information se rapportant à une personne physique identifiée ou identifiable ». Ainsi énoncée, la notion paraît couvrir les informations liées à une personne, telles que son nom, prénom,

---

[112] Cette formulation s'inspire de l'expression utilisée par le ministre suisse de la santé, Monsieur Alain Berset, pendant la pandémie de Covid19, v. D. Rochebin, V. Gillio et F. Boillat, « Alain Berset, un ministre omniprésent à l'épreuve du déconfinement », *RTS* 20 avr. 2020.

[113] J. Frayssinet, *Informatique fichiers et libertés,* Litec, 1992, n° 81, p. 34.

[114] V. par ex. J. Frayssinet, *Informatique fichiers et libertés,* Litec, 1992, n° 82, p. 35 ; G29, WP 136, Avis 4/2007 du groupe de travail relatif au concept de données à caractère personnel, 20 juin 2007, p. 4 ; F. Lesaulnier, « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz IP/IT* 2016, p. 573 ; *JCl. comm.,* fasc. 930, « Données à caractère personnel. Introduction générale et champ d'application de la règlementation relative à la protection des données personnelles », par R. Perray, 2019 (actu. 2020), n° 90.

[115] Pour une étude de la différence entre la notion d'information nominative et celle de donnée personnelle, v. J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 53 s.

numéro de sécurité sociale, sa profession, mais aussi son image, sa voix ou encore son sexe. Personne n'oserait contester la qualification de donnée à caractère personnel pour ces données. Mais qu'en est-il lorsque les données sont plus éloignées des personnes et que leur rattachement n'est possible qu'à l'occasion d'un traitement particulier ? Par exemple, une heure, un numéro d'appareil, ou des coordonnées géographiques relèvent-ils de la notion de donnée à caractère personnel ? *Prima facie,* rien ne permet de déceler, dans ces données, un rapport avec une personne physique. Pourtant, lorsque cette heure révèle le moment de la connexion de l'utilisateur à un site Internet, lorsque ce numéro d'appareil dévoile l'instrument utilisé ou lorsque ces coordonnées géographiques trahissent le lieu de la connexion, ces données se rapportent bien à une personne physique[116]. Bien sûr, personne n'oserait affirmer que, par nature et de manière abstraite, une heure, un numéro d'appareil ou une donnée géographique se rapportent à un individu. Pour autant, de plus en plus de traitements effectués sur ces données font apparaître un tel rapport, déclenchant ainsi la qualification de donnée à caractère personnel.

L'évolution de la notion est donc tributaire des développements techniques. À cet égard, deux facteurs contribuent indéniablement à l'extension de la notion. D'une part, l'augmentation considérable du nombre de données générées à chaque instant, et d'autre part, le décuplement et la généralisation des capacités de traitement. Ces facteurs ont été théorisés au sein des fameuses conjectures de Moore relatives à l'évolution de la puissance des ordinateurs[117]. Selon Gordon Moore, la complexité et la densité des transistors, c'est-à-dire l'élément principal composant les processeurs des ordinateurs, doubleraient tous les deux ans[118]. La puissance des appareils suivrait la même courbe, permettant ainsi de traiter des informations de plus en plus rapidement. L'avantage de ces évolutions est la diminution, à la même échelle, du coût du stockage des informations. Ces facteurs ont donc favorisé l'augmentation de la collecte de données laquelle, cumulée à la diversification des données générées, permet la mise en œuvre de recoupements révélant des liens entre les données et les personnes. Ces

[116] Sur cette question, à propos des informations pouvant être inférées à partir de l'envoi de courriers électroniques (*email*), v. déjà, E. Andrieu, « Internet et la protection des données personnelles », *Legicom* 2000, nº 21-22, p. 155, spéc. p. 162.
[117] G. Moore, « Cramming more components onto integrated circuits », *Electronics* 1965, vol. 38, nº 8 ; G. Moore, « Progress in digital integrated electronics », *Institute of Electrical and Electronics Engineers* 1975, p. 11.
[118] Ces conjectures se sont révélées exactes pendant de nombreuses années. Il est aujourd'hui possible de constater un ralentissement de la cadence des évolutions prédites.

évolutions ont encouragé une acception large de la notion de donnée à caractère personnel.

26. Questionnements sur l'étendue de la notion. Si toute donnée peut désormais relever de la qualification de donnée à caractère personnel, comment distinguer les données qui doivent recevoir une protection juridique de celles qui doivent circuler librement ? Questionner l'effectivité de la notion de donnée à caractère personnel revient donc à s'intéresser à l'effet produit par l'expansion de la notion sur la protection des personnes. Dans cette démarche, il semble important de s'assurer que cette expansion garantit une meilleure protection des personnes et qu'elle n'empiète pas indûment sur d'autres libertés. Il est certain que faire entrer toutes les données dans le domaine du droit des données à caractère personnel servirait difficilement la protection des personnes. Non seulement les atteintes les plus graves seraient mises sur un pied d'égalité avec les atteintes seulement potentielles, mais les informations trop éloignées des personnes ne pourraient plus circuler librement, faisant ainsi chanceler d'autres libertés telles que les libertés d'expression ou d'information.

Pour autant, la notion de donnée à caractère personnel n'est que la porte d'entrée de cette matière, laquelle présente assurément un régime complexe.

27. Justification d'une approche restreinte des règles étudiées. Composés chacun d'une centaine d'articles, le règlement européen 2016/679 et la loi Informatique et libertés prévoient un enchevêtrement de normes et d'acteurs rendant leur appréhension malaisée[119]. Toutes ces règles n'ont pas les mêmes implications en matière de protection des personnes : seules certaines d'entre elles requièrent une analyse détaillée. Au cœur de celles-ci se trouvent indiscutablement les conditions de licéité des traitements de données à caractère personnel. Ces conditions représentent les fondations sur lesquelles repose le traitement, puisque leur entorse entraîne l'illicéité du traitement. Elles sont donc essentielles, tant pour la sécurité juridique des traitements que pour la protection des personnes. D'autres règles telles que le principe

[119] C. Castets-Renard, « Brève analyse du règlement général relatif à la protection des données personnelles », *Dalloz IP/IT* 2016, p. 331. Pour une analyse des spécificités du droit français des données à caractère personnel au regard du règlement européen n° 2016/679, N. Martial-Braz et J. Rochfeld (dir.), *Droit des données personnelles. Les spécificités du droit français au regard du RGPD,* Dalloz, 2019. Sur le volume excessif des règles de nature à nuire à leur réception, v. J. Carbonnier, *Droit et passion du droit sous la V^e^ République,* Flammarion, 1996, p. 75 s.

de minimisation, ou les accès par les tiers, doivent également être étudiées. Ces règles sont d'autant plus importantes qu'elles influencent les données à la disposition des organismes, et donc les données pouvant être traitées à des fins de réidentification.

En revanche, les règles liées à la logique de responsabilité, notamment celles relatives aux codes de conduite, à la certification ou aux analyses d'impact ainsi que les nouveaux droits reconnus aux personnes[120] requièrent des développements plus superficiels. La raison principale réside dans la jeunesse de ces nouvelles règles, laquelle empêche une mesure juste de leur effectivité. Ces règles sont issues du changement de paradigme mis en place par le règlement européen et entrées en application en 2018. Ce texte repose sur une logique de responsabilité renvoyant aux organismes le soin d'évaluer leurs pratiques et d'instaurer des procédures internes de protection des données[121]. Pour autant, ces règles feront tout de même l'objet d'analyses incidentes, notamment à l'occasion de l'étude de la mise en œuvre de la protection, laquelle appelle d'importants développements.

28. Les difficultés de mise en œuvre de la protection. La faible mise en œuvre du droit des données à caractère personnel, tant par les acteurs spécialisés que par les juridictions de droit commun, remet en question l'effectivité de la matière. Pendant longtemps, le droit des données à caractère personnel a plutôt fait l'objet d'une application lacunaire, et des traitements illicites ont pu prospérer. De telles illicéités laissent supposer une protection ineffective des personnes par le droit des données personnelles. L'entrée en application du règlement européen a entraîné une prise de conscience du grand public et des organismes de la nécessité de protéger plus efficacement les données[122]. Pour conforter ce mouvement, le présent travail s'intéressera aux modalités de mise en œuvre du droit des données à caractère personnel. En définitive, plusieurs propositions seront formulées dans le but d'améliorer le système de contrôle et celui de sanction. Certaines d'entre elles sont

[120] Sur les nouveaux droits consacrés par le règlement européen, v. not. L. Cluzel-Métayer et E. Debaets, « Le droit de la protection des données personnelles : la loi du 20 juin 2018 », *RFDA* 2018, p. 1101 ; N. Martial-Braz, « Le renforcement des droits de la personne concernée », *Dalloz IP/IT* 2017, p. 253.
[121] Dans le domaine de la sécurité informatique, une étude a montré que l'obligation de prendre en compte, de manière explicite, les aspects de sécurité dans les documents officiels et spécifications techniques d'Internet (*request for comments*) a eu des effets très positifs sur la sécurité de manière générale, v. J. Whitaker, B. Reaves, S. Prasad et W. Enck, « Thou shalt discuss security : quantifying the impacts of instructions to RFC authors », *SSR '19* nov. 2019, p. 57.
[122] CNIL, « 1 an de RGPD : une prise de conscience inédite », 23 mai 2019.

destinées à renforcer l'indépendance de la CNIL et la transparence de ses activités[123]. D'autres propositions visent à diversifier les contrôles, notamment en renforçant la place des experts techniques au sein des organismes et en augmentant les collaborations entre les autorités de contrôle et entre les pays. Enfin, et pour encourager les recours en responsabilité en cas de traitements fautifs de données à caractère personnel, certaines évolutions sont apparues nécessaires. D'un point de vue purement procédural, il convient de faciliter les actions collectives. En effet, le caractère commun et partagé des atteintes résultant des traitements de données appelle une défense collective[124]. Ensuite, la nature des atteintes engendrées par ces traitements, particulièrement sur la liberté individuelle, commande un renforcement de la place du juge judiciaire[125]. En sus, pour faciliter la mise en œuvre des actions juridictionnelles, il est apparu nécessaire de consacrer une présomption simple de faute à l'encontre de l'organisme traitant les données personnelles et de proposer une nomenclature des préjudices pouvant résulter de ces traitements[126]. Toutes ces évolutions permettront de renforcer l'effectivité de la protection des personnes.

§ II. Méthode retenue

29. Une étude de droit français éclairée par le droit européen. L'analyse du droit français constituera naturellement notre principal outil de travail. Dans le domaine des données personnelles, les règles nationales sont largement enrichies par des sources européennes[127]. Ainsi, la présente étude ne se bornera pas à explorer la loi, la jurisprudence et la doctrine françaises, mais sera étendue à l'analyse des textes européens applicables en la matière, particulièrement la directive 95/46 remplacée par le règlement 2016/679, ainsi que leurs interprétations jurisprudentielles et doctrinales[128]. À ces textes européens s'ajoute l'apport des sources supranationales, particulièrement celles issues du droit du Conseil de l'Europe. Ainsi, l'article 8 de la Convention européenne des droits de l'homme et son interprétation seront régulièrement visés. Ce corpus apporte souvent un éclairage pertinent sur les évolutions

[123] V. *infra*, n^os^ 477 s.
[124] V. *infra*, n^os^ 533 s.
[125] V. *infra*, n^os^ 529 s.
[126] V. *infra*, n^os^ 562 s. et n^os^ 572 s.
[127] Art. 55 de la Constitution du 4 août 1958
[128] N. Martial-Braz et J. Rochfeld (dir.), *Droit des données personnelles. Les spécificités du droit français au regard du RGPD,* Dalloz, 2019, n^o^ 104, p. 15 s.

de la matière[129]. Ces normes sont également complétées par les sources du droit souple[130], particulièrement abondantes dans le droit des données à caractère personnel. Ainsi, l'étude des avis, recommandations et délibérations, notamment adoptés par les autorités de contrôle, ne sera pas négligée.

L'étude de cette matière requiert également une appétence particulière pour des domaines juridiques variés ainsi qu'un intérêt pour le droit comparé.

30. Une étude éclairée par d'autres branches du droit. D'emblée, il apparaît que le droit des données à caractère personnel entretient d'importants rapports avec la plupart des branches du droit. À titre d'exemple, le droit des données à caractère personnel concerne directement le droit civil. La protection des données personnelles est souvent mise en perspective avec le droit au respect de la vie privée. Selon certains auteurs, cette protection ne serait d'ailleurs rien d'autre que « l'une des déclinaisons contemporaines les plus importantes » de ce droit[131]. Le droit des données à caractère personnel entretient aussi des liens avec le droit des contrats[132]. D'un côté, le droit des données à caractère personnel enrichit le droit des contrats. À ce titre, certains auteurs considèrent qu'il en serait une source nouvelle[133], et la décision du 25 juin 2013 de la chambre commerciale de la Cour de cassation est illustrative de cet enrichissement de la matière contractuelle. La Cour de cassation a reconnu qu'un fichier contenant des données à caractère personnel n'ayant pas été déclaré auprès de la Commission nationale de l'informatique et des libertés (ci-après CNIL) était une chose hors commerce[134]. Le manquement à l'une des formalités instaurées par le droit des données

---

[129] Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, *Manuel de droit européen en matière de protection des données 2018*, Office des publications de l'Union européenne, 2019, p. 20 s.

[130] L'étude du Conseil d'État relative au droit souple le définit comme « l'ensemble des instruments réunissant trois conditions cumulatives : ils ont pour objet de modifier ou d'orienter les comportements de leurs destinataires en suscitant, dans la mesure du possible, leur adhésion ; ils ne créent pas par eux-mêmes de droits ou d'obligations pour leurs destinataires ; ils présentent, par leur contenu et leur mode d'élaboration, un degré de formalisation et de structuration qui les apparente aux règles de droit », v. Conseil d'État, « Le droit souple », *Rapport Public 2013*, La Documentation française, 2013, p. 61. Pour s'en convaincre, il suffit de parcourir le sommaire des actes du colloque « Le droit souple » du 27 mars 2008, organisé par l'Association Henri Capitant, v. *Travaux de l'Association Henri Capitant*, « Le droit souple », t. 13, Journées nationales, Dalloz, 2009.

[131] S. Veil (dir.), « Redécouvrir le Préambule de la Constitution. Rapport au président de la République », La Documentation française, déc. 2008, p. 71. En écho à la formule de Jhering, selon laquelle la possession est « le bastion avancé de la propriété », le droit des données personnelles serait, à l'ère numérique, le bastion avancé de la vie privée, v. en ce sens E. Netter, *Numérique et grandes notions du droit privé. La personne, la propriété, le contrat*, mémoire en vue de l'habilitation à diriger des recherches en droit privé, Picardie, 20 nov. 2017, n° 60, p. 83.

[132] Sur cette question, v. la richesse des contributions produites à l'occasion de la journée d'étude *Contrat & protection des données à caractère personnel* de l'Université Caen Normandie, Caen, 22 mars 2019, *AJ Contrat* 2019, p. 366 s. et p. 421 s.

[133] J. Rochfeld, « Une nouvelle source en droit des contrats : la loi Informatique et libertés », *RDC* 2014, n° 1, p. 119, § 4.

[134] Cass. com., 25 juin 2013, n° 12-17.037, *Bull.* 2013, IV, n° 108.

à caractère personnel était ainsi considéré comme une cause d'illicéité de l'objet du contrat. De l'autre, le droit des contrats s'est emparé du droit des données à caractère personnel, en imposant *de facto* l'application de ses dispositions. Les exemples sont nombreux et pourraient être multipliés : les relations entre le responsable du traitement et son sous-traitant doivent être formalisées dans un contrat écrit[135], le contrat figure parmi les conditions de licéité du traitement, les conditions générales d'utilisation des services en ligne et les politiques de confidentialité sont qualifiées de contrat[136].

Le droit des données à caractère personnel cultive également d'importants rapports avec la responsabilité civile puisque son régime renvoie aux règles classiques de la responsabilité civile extracontractuelle[137].

Néanmoins, ces rapports ne se limitent pas au droit civil, ils touchent également de nombreuses autres matières du droit privé telles que le droit de la consommation[138], le droit pénal[139], le droit de la concurrence[140], le droit des marchés financiers[141], la propriété intellectuelle[142]. Si notre étude sera principalement orientée autour du droit privé, puisque ce domaine est déjà très large, des analyses ponctuelles de certaines matières du droit public, notamment le contentieux administratif[143] ou l'accès aux documents administratifs[144], seront effectuées toutes les fois où l'analyse de la protection des personnes le justifiera.

La mise en perspective et la confrontation du droit des données avec ces autres matières sont nécessaires pour analyser la réalité de l'effet produit par le droit des données et éventuellement en proposer certaines modifications.

---

[135] F.-L. Simon et A. Bounedjoum, « RGPD : quelles règles en matière de responsabilité et quels impacts sur les contrats ? », *AJ Contrat* 2018, p. 172.
[136] G. Loiseau, « La valeur contractuelle des conditions générales d'utilisation des réseaux sociaux », *CCE* 2012, nº 7-8, comm. 78.
[137] Art. 82 du règlement UE nº 2016/679.
[138] D. Lebeau-Marianna et A. Balducci, « UFC – Que Choisir contre Google + : la loi Informatique et libertés, un moyen supplémentaire de protection du consommateur ? », *Dalloz IP/IT* 2019, p. 258.
[139] Par exemple, le code pénal consacre un chapitre entier aux « atteintes aux systèmes de traitement automatisé de données », v. not. art. 323-1 s. de ce code.
[140] Par exemple, les acquisitions d'entreprise entraînent des questions relatives à la gestion des données entre les entreprises, v. not. CNIL, décision nº 2017-075 du 27 nov. 2017, mettant en demeure la société WhatsApp.
[141] Par exemple, le code monétaire et financier consacre un chapitre aux « services de communication de données », v. art. L. 323-1 s. de ce code.
[142] Par exemple, la propriété intellectuelle protège les bases de données, v. la directive CE nº 96/9 du Parlement européen et du Conseil du 11 mars 1996 concernant la protection juridique des bases de données, *JOUE* 27 mars 1996, L-77/20, p. 20 s., et les arrêts de la CJUE sur ce thème, v. not. CJUE, 9 nov. 2004, *The British Horseracing Board Ltd et autres* c. *William Hill Organization Ltd*, C-203/02, § 29 s.
[143] Par exemple, le Conseil d'État connaît des recours pour excès de pouvoir et de pleine juridiction contre les décisions de la CNIL, v. *infra*, nº 525.
[144] Par exemple, l'article L. 312-1-2 du code des relations entre le public et l'administration encadre la mise à la disposition du public de documents comportant des données à caractère personnel.

31. Une étude éclairée par le droit comparé. Dans l'objectif qui est le nôtre de proposer des améliorations du droit européen des données à caractère personnel, l'éclairage ponctuel du droit comparé semble particulièrement pertinent[145]. Seulement, nous n'avons pas l'ambition de traiter conjointement en droit français et dans plusieurs autres droits la question de la protection des personnes par le droit des données à caractère personnel. Cet exercice serait particulièrement complexe, et son intérêt relatif. Complexe d'abord parce que, même si le droit européen des données à caractère personnel a une vocation universaliste, la réalité de la mise en œuvre des principes européens dans d'autres pays appelle d'importantes précautions[146]. Relatif ensuite parce que la conception de ce que doit être la protection des personnes est loin d'être universelle. Elle dépend des cultures et des histoires propres à chaque pays, lesquelles engendrent une conception différente de l'intimité, de la vie privée et de la place des personnes dans la société[147]. Par exemple, l'Europe garde sans doute une mémoire plus vive des atrocités perpétrées pendant la Seconde Guerre mondiale que d'autres régions. Il est admis que la collecte de données personnelles et l'élaboration de fichiers ciblant certaines minorités ou certains types de populations y ont fortement contribué[148]. Ainsi, les Européens ont une aversion, ou au moins une défiance, à l'égard des fichiers de noms[149]. Les différents États ont donc élaboré des règles de protection conformes à leurs histoires et aux attentes de leurs citoyens[150]. Aussi, plutôt que de butiner dans les différents droits nationaux, au risque de ne pas prendre le temps de comprendre les

---

[145] R. Sacco, *La comparaison juridique au service de la connaissance du Droit*, Economica, 1991, nº 2, p. 8 s.

[146] Pour une analyse très complète des effets dans l'espace du règlement européen, v. M. Mantovani, « Le RGPD en tant qu'espace juridique multi-échelle : quelles implications pour le droit international privé ? », *Revue de Droit International d'Assas* 2019, nº 2, p. 63 ; v. aussi A.-T. Norodom, « Le standard européen de protection des données au regard du droit international », *Le règlement général sur la protection des données. Aspects institutionnels et matériels*, dir. B. Brunessen et A. Bensamoun, Mare et Martin, 2020, p. 154 s.

[147] X. Bioy, « Le libre développement de la personnalité en droit constitutionnel, essai de comparaison Allemagne, Espagne, France, Italie, Suisse », *RID comp.* 2003, vol. 55, nº 1, p. 123, spéc. p. 125 s. En matière de droits de l'homme, malgré un consensus commun, les différences propres aux États ont de l'importance, v. M. Mutua, « The ideology of human rights », *Virginia Journal of International Law* 1996, vol. 36, p. 589 s. [36 VA. J. INT'L L. 589].

[148] Comme le remarquait Monsieur Pierre-Henri Prélot, « la mémoire douloureuse du fichage des Juifs et de l'obligation du port de l'étoile jaune, préludes à la déportation massive, ont longtemps fait peser en France, après 1945, une méfiance extrême à l'encontre de tout procédé permettant la conservation de renseignements personnalisés », P.-H. Prélot, *Droit des libertés fondamentales*, 2e éd., Hachette Supérieur, 2010, nº 462, p. 188.

[149] B. Dumont, « La régulation à l'échelle communautaire, une analyse économique des instruments et institutions de la protection des données au sein de l'UE », *Réseaux* 2011, nº 3, vol. 167, p. 49.

[150] Pour un exposé sommaire de ces divergences, v. not. J. Whitman, « The two western cultures of privacy : dignity versus liberty », *The Yale Law Journal* 2004, vol. 113, p. 1151 s. [113 YALE L.J. 1151] ; P. Schwartz et K.-N. Peifer, « Transatlantic data privacy », *Georgetown Law Journal* 2017, vol. 106, p. 115 s. [106 GEO. L.J. 115] et J.-L. Halpérin, « Protection de la vie privée et privacy : deux traditions juridiques différentes ? », *Les Nouveaux Cahiers du Conseil constitutionnel* 2015, nº 48, p. 59. Pour une analyse de l'approche de la vie privée en fonction des États, I. Altman, « Privacy regulation : culturally universal of culturally specific ? », *Journal of social issues* 1977, vol. 33, p. 67 s.

raisons et l'argumentation qui soutiennent ces règles[151], nous avons choisi de ne recourir au droit comparé que lorsqu'une telle perspective était nécessaire. À cet effet, nous avons puisé nos références dans les deux grandes familles de droit : les droits de *common law* et les droits romano-germaniques. Au sein de la première famille de droit, c'est plutôt le droit des États-Unis d'Amérique qui sera évoqué, en raison de sa singularité et de sa fréquente confrontation avec le modèle européen[152]. Cette perspective apparaît d'autant plus nécessaire que le nombre de services numériques proposés par des entreprises américaines est important. Dans cette démarche, il est impératif de rappeler qu'il n'existe pas « un » modèle américain de protection des données personnelles, mais plutôt un ensemble composite et hétérogène construit autour de règles issues des droits étatiques et du droit fédéral[153]. Cette hétérogénéité rend les comparaisons avec le modèle européen particulièrement périlleuses et invite donc à la prudence. Quant à la seconde famille de droit, c'est-à-dire celle des droits romano-germaniques, nous nous concentrerons évidemment sur le droit français et utiliserons le droit allemand, italien ou suisse notamment pour éprouver nos analyses.

32. Thèse défendue. Il est courant d'affirmer que la notion de donnée à caractère personnel *doit* être interprétée largement. Les arguments favorables à cette conception sont connus : une interprétation extensive serait nécessaire face au nombre et à la variété des données dessinant les traits, plus ou moins épais, du portrait des personnes. *A priori,* cette expansion du domaine assure une meilleure protection des individus et participe donc à son effectivité. Pour autant, en va-t-il vraiment toujours ainsi ? Cette expansion n'engendrerait-elle pas des conséquences négatives ? En matière de données personnelles, et comme le remarquait Jean Foyer, « il faut se souvenir du proverbe : "Qui trop embrasse mal étreint" »[154]. L'application très large de la notion de donnée à caractère personnel n'a pas toujours les bénéfices escomptés. Au contraire, cette application étendue empiète sur d'autres libertés individuelles également nécessaires

---

[151] C. Atias, *Épistémologie juridique,* PUF, 1985, n^os^ 91 s., p. 63 s.
[152] C. Castets-Renard, « Quels liens établir entre les USA et l'UE en matière de vie privée et protection des données personnelles ? », *Dalloz IP/IT* 2016, p. 115 ; P. Schwartz et D. Solove, « Reconciling personal information in the United States and European Union », *California Law Review* 2014, vol. 102, p. 877 s. [102 CALIF. L. REV. 877].
[153] P. Schwartz et D. Solove, *Information privacy law*, 6^e^ éd., Wolters Kluwer, 2018, p. 2, « Information privacy law is an interrelated web of tort law, federal and state constitutional law, federal and state statutory law, evidentiary privileges, property law, contract law, and criminal law », pouvant être traduit par « la protection des données personnelles est une toile composée de responsabilité civile, de droit constitutionnel étatique et fédéral, de lois étatiques et fédérales, de règles de procédure, de droit des biens, de droit des contrats et de droit pénal ».
[154] J. Foyer, 1^re^ séance du mardi 4 oct. 1977, *JORF AN* 5 oct. 1977, n^o^ 79, p. 5783.

pour une protection effective des personnes. Afin d'éviter ces effets non désirés, un nouveau critère d'encadrement notionnel doit être formulé. Celui-ci s'inscrit dans la logique actuelle de responsabilité des organismes traitant les données.

Pour accompagner l'encadrement du domaine des données à caractère personnel, une consolidation du régime doit être formulée. Les règles issues de ce droit se révèlent insuffisantes pour protéger efficacement les personnes contre des traitements de plus en plus intrusifs. Il s'avère en effet que les traitements de données exposent les personnes à des manipulations les empêchant de développer librement leur personnalité. Dès lors, pour garantir un effet réel sur la protection des personnes, certains principes du droit des données à caractère personnel doivent évoluer. Enfin, l'effectivité de la protection des personnes se mesure également par l'étude de la mise en œuvre du droit des données personnelles. En dépit d'une pluralité d'acteurs impliqués, celle-ci apparaît lacunaire et insuffisante. L'amélioration de la mise en œuvre de ce droit passe donc par un renforcement des contrôles internes et externes et par une simplification des conditions permettant d'engager la responsabilité des organismes.

33. Plan de l'étude. Le plan retenu reprend directement ces idées. Pour sonder l'effectivité de la protection des personnes, il faut d'abord s'intéresser à l'étendue du droit des données à caractère personnel. Dans cette démarche, l'analyse de la notion de donnée à caractère personnel s'avère nécessaire. À l'étude, il apparaît que celle-ci « s'étend, et s'enfle, et se travaille »[155], pour emporter dans son sillon un nombre croissant de données. Pour éviter que le domaine « crève » par excès d'application, il convient de modérer cette expansion.

Sonder l'effectivité de la protection des personnes demande ensuite de s'intéresser au régime applicable aux données à caractère personnel. L'abondance de règles dans cette matière encourage à diriger notre étude vers celles qui ont un effet réel sur la protection des personnes. Animée par cette volonté, nous proposerons de consolider certains des principes et d'améliorer la mise en œuvre du droit des données à caractère personnel dans l'objectif de renforcer la protection des personnes. Notre travail se révèle donc comme un plaidoyer en faveur de la protection des personnes.

---

[155] « Une Grenouille vit un Bœuf, […] Envieuse s'étend, et s'enfle, et se travaille » mais la grenouille « S'enfla si bien qu'elle creva », J. de La Fontaine, *Choix de fables de La Fontaine,* 22e éd., Delalain, 1878, p. 2.

Après avoir démontré pourquoi il est nécessaire d’encadrer l’expansion du domaine des données à caractère personnel (Première partie) il conviendra de s’attacher à renforcer le régime applicable à ces données (Deuxième partie).

Première partie – Encadrer le domaine des données à caractère personnel

Deuxième partie – Renforcer le régime des données à caractère personnel

PREMIÈRE PARTIE – ENCADRER LE DOMAINE DES DONNÉES À CARACTÈRE PERSONNEL

34. Une société informatisée. L'essor et le progrès constants des techniques de l'informatique et des communications ont participé à une numérisation de nos modes de vie, de nos modes de production et de nos interactions sociales. Cette numérisation va de pair avec une explosion du nombre de traitements de données : les entreprises veulent gagner en productivité, les météorologues désirent mieux prédire le temps, les individus souhaitent communiquer plus rapidement. Si les usages et les objectifs de ces traitements sont divers, ils partagent tous un point commun : les données.

Les données sont disponibles en quantité toujours croissante, difficiles à protéger et faciles à reproduire ; elles ont la particularité de ne pas s'épuiser lorsqu'on les utilise[156]. Elles innervent nos sociétés ; elles nous aident à choisir la route la plus rapide pour aller dans notre restaurant favori, elles nous permettent d'accéder aux photos de notre famille éloignée, elles nous aident à choisir notre hôtel lors d'un voyage. Les usages sont multiples et les régimes juridiques associés sont tout aussi divers.

35. Un encadrement juridique. Le droit n'est pas en reste face aux changements apportés par l'informatique et le numérique à nos sociétés. Ces évolutions sont d'une telle ampleur que certains auteurs n'ont pas hésité à qualifier le développement des technologies numériques de « troisième révolution industrielle »[157]. Face à ces évolutions, le juriste se demande immédiatement comment le droit doit appréhender ces nouveaux domaines. Trois approches juridiques semblent envisageables. La première consiste à considérer que le droit commun[158] est impuissant à réguler ces évolutions ; le législateur doit alors être sollicité pour édicter de nouvelles règles

[156] L.-D. Benyayer et S. Chignard, *Datanomics. Les nouveaux business models des données*, FYP, 2015, p. 37.
[157] J. Rifkin, *La troisième révolution industrielle*, Actes sud, 2013.
[158] Selon Monsieur Nicolas Balat, « le droit commun désigne les règles juridiques au domaine d'application indéfini […] il est, par essence, potentiellement applicable à tous les cas qui se présentent » pour une institution donnée, N. Balat, *Essai sur le droit commun*, th. Paris II, 2014, LGDJ, n° 243, p. 149.

spéciales, mieux adaptées à ces phénomènes[159]. La seconde approche consiste à poser comme hypothèse que le droit commun peut répondre à la majorité des problématiques créées par ces nouveaux phénomènes, sans qu'il soit nécessaire d'adopter des règles spéciales[160]. Enfin, la troisième approche est une sorte de voie médiane entre les deux approches précédentes, favorisant l'adoption d'un régime mixte. En d'autres termes, il faut se demander si les règles classiques sont suffisantes pour répondre aux enjeux liés à l'informatique et à la mise en réseau des ordinateurs[161].

36. Un champ d'application très large de la donnée. D'un point de vue étymologique, le terme donnée provient du latin *datum*, « ce qui est donné ». Dans le langage courant, la donnée est aujourd'hui définie comme une « représentation conventionnelle d'une information (fait, notion, ordre d'exécution) sous une forme (analogique ou digitale) permettant d'en faire le traitement automatique »[162]. À première vue, la notion de donnée semble comparable à celle d'information[163]. Pourtant, le numérique a tant modifié les méthodes de collecte, de traitement et de transmission des données que ces notions présentent quelques différences. Aujourd'hui, les données sont souvent enregistrées directement en code numérique et l'humain peut, à l'aide ou non d'algorithmes informatiques, leur donner du sens en les contextualisant ou en les interprétant[164]. Contrairement aux époques précédentes, les données peuvent faire l'objet de traitements d'une telle ampleur qu'elles sont désormais une matière première de l'information[165].

---

[159] Comme le remarquait Pierre Catala, « le propre des législations spécifiques est d'avoir un objet particulier et non pas universel. Elles laisseront toujours subsister, à la périphérie des monopoles d'exploitation, des informations dépourvues de protection privatives », v. P. Catala, « La "propriété" de l'information », in *Mélanges P. Raynaud*, Dalloz, 1985, p. 97 s., n° 27, spéc. p. 108.

[160] N. Mathey, « L'uberisation et le droit des contrats : l'immixtion des plateformes dans la relation contractuelle », colloque *Le droit civil à l'ère du numérique* du Master 2 Droit privé général et du laboratoire de droit civil de l'Université Paris II Panthéon Assas, Paris, 21 avr. 2017, LexisNexis, p. 9.

[161] Madame Judith Rochfeld a proposé de s'interroger sur l'insertion dans le code civil « des principes de réappropriation, par les individus, de leur personnalité captée à leur insu », v. J. Rochfeld, « La vie tracée ou le code civil doit-il protéger la présence numérique des personnes ? », in *Mélanges J. Hauser*, LexisNexis et Dalloz, 2012, p. 619 s., n° 3, spéc. p. 622 et n^{os} 11 s., spéc. p. 630 s.

[162] A. Rey et J. Rey-Debove, *Le petit Robert de la langue française*, 2017, Le Robert, *V°* « Donnée », sens 2. L'Académie française définit la donnée comme la « représentation d'une information sous une forme conventionnelle adaptée à son exploitation », v. *Dictionnaire de l'Académie française*, 9e éd., *V°* « Donnée », sens 4.

[163] La notion d'information est particulièrement large, v. *L'information en droit privé : travaux de la conférence d'agrégation*, dir. P. Lagarde et Y. Loussouarn, LGDJ, 1978.

[164] C'est tout l'objet du domaine des sciences de la donnée, lequel peut être défini comme « un ensemble de techniques qui vise à extraire la valeur des données », V. Kotu et B. Deshpande, *Data science. Concepts and practice,* 2e éd., Morgan Kaufmann, 2018, p. 1.

[165] Comp. F. Lesaulnier, *L'information nominative,* th. Paris II, 2005, n° 16, p. 30.

37. La nature des données. Les données peuvent porter sur une infinité d'objets ; relatives à des lieux, liées à des animaux ou associées à des produits, les données sont partout. Lorsqu'elles peuvent être rattachées à des personnes physiques, elles sont qualifiées de *données à caractère personnel*.

38. Une évolution notionnelle. Sollicitée quotidiennement, la notion de donnée à caractère personnel doit s'adapter pour répondre aux besoins d'une société dans laquelle les personnes se dévoilent de plus en plus. La loi du 6 janvier 1978 avait consacré la notion d'information nominative[166]. Celle-ci, jugée trop restreinte, a été remplacée en 2004 par celle de donnée à caractère personnel[167]. Ce glissement sémantique est principalement lié aux évolutions technologiques qui permettent d'établir plus facilement des liens entre une donnée et un individu[168]. Par exemple, au début des années 1980, il était encore difficile de penser que des données géographiques permettraient, un jour, de réidentifier une grande partie de la population. Pourtant, dans une étude publiée en 2013, quatre chercheurs montraient, après avoir analysé des données de déplacements sur quinze mois, que quatre points spatio-temporel suffisent à réidentifier 95 % des utilisateurs d'un *smartphone*[169].

39. Des risques d'application généralisée de la notion. À première vue, l'extension de la notion permet d'assurer une protection étendue des individus contre des traitements de plus en plus indirects et de plus en plus intrusifs ; c'est une protection plus complète qui semble ainsi voir le jour. Cette extension paraît pertinente compte tenu du développement des mesures d'identification indirecte[170]. Elle permet en effet de soumettre à la loi des traitements dont les données n'auraient pas de lien apparent avec une personne mais pour lesquels, grâce à des recoupements ou des informations externes, un rattachement serait possible permettant ainsi d'obtenir des renseignements sur une personne.

---

[166] Art. 4 de la loi nº 78-17 du 6 janv. 1978.
[167] G. Gouzes, « Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », Assemblée nationale, nº 3526, 9 janv. 2002, p. 17.
[168] G. Braibant, « Données personnelles et société de l'information. Rapport au Premier ministre sur la transposition en droit français de la directive nº 95/46 », La Documentation française, 1998, p. 45.
[169] Y.-A. de Montjoye, C. Hidalgo, M. Verleysen et V. Blondel, « Unique in the Crowd: The privacy bounds of human mobility », *Scientific Reports* 2013, nº 1376, p. 2.
[170] A. Türk, « Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », Sénat, nº 218, 19 mars 2003, p. 47.

Passée cette première impression, il semble tout de même nécessaire de vérifier les contours du champ d'application de la notion. Il serait regrettable d'appliquer une sorte de principe de précaution à toutes les données puisque celui-ci risquerait d'empêcher la circulation d'informations sans lien avec des personnes. S'il est parfaitement naturel de souhaiter que la notion de donnée à caractère personnel s'adapte aux nouveaux usages et aux technologies, il faut éviter qu'elle devienne si large qu'elle s'appliquerait, *de facto*, à toutes les données. En effet, le risque d'une interprétation *in abstracto* de ces termes est de voir reconnaître à toutes les données l'attribut de « caractère personnel ».

40. Les effets éventuels. Comme le remarquait Philippe Malaurie, « chaque changement dans l'étendue, la raison d'être et le régime des droits de la personnalité, ne porterait-il que sur des détails anecdotiques, en modifie la signification, parfois de façon imperceptible. Chaque détail compte. Un droit n'est pas seulement fait de principes ou de règles générales, mais aussi de leurs modalités qui, seules, leur donnent un sens concret et quotidien. Modifiez l'une, tout est transformé »[171]. Le constat de l'expansion de la notion amène à s'interroger sur ses effets : protège-t-elle vraiment mieux les personnes ? Cette extension ne risquerait-elle pas de diluer la protection des informations les plus personnelles et d'avoir des effets négatifs sur certaines libertés individuelles ? Par exemple, si l'on considère abstraitement qu'un point géographique peut devenir donnée à caractère personnel, ne risque-t-on pas de réduire le nombre d'informations géographiques pouvant circuler librement ? Une telle restriction ne risque-t-elle pas de réduire la liberté d'information et d'expression sur ces sujets ? Voici quelques-unes des questions auxquelles il s'agira de répondre et qui aideront à comprendre pourquoi un nouveau critère de définition de la donnée à caractère personnel doit voir le jour.

41. Pour une acception limitée de la notion de donnée à caractère personnel. La généralité de la notion de donnée à caractère personnel permet de faire appliquer la loi à des données dont le lien avec une personne physique n'est pas toujours certain ou n'est que potentiel. Une telle conception risque en pratique d'entraîner une application

[171] P. Malaurie, « Les droits de la personnalité en 2003 », *Mélanges A. Decocq,* Litec, 2004, p. 468 s., nº 4, spéc. p. 470.

hégémonique de la notion de donnée à caractère personnel au détriment de sa cohérence et de son effectivité[172]. Pour éviter une telle application, tout en anticipant les possibles contournements, il convient de cantonner l'expansion de la notion de donnée à caractère personnel. Cet encadrement n'est pertinent que pour les données indirectement identifiantes puisque c'est pour celles-ci que le lien avec la personne peut être si lointain et si incertain que l'atteinte à la personne n'est pas seulement éventuelle mais est indéterminée.

42. Plan. Depuis l'adoption en 1978 de la loi relative à l'informatique, aux fichiers et aux libertés, la notion de donnée à caractère personnel n'a cessé de s'étendre (Titre I). Pour éviter une application hégémonique de la notion, il convient d'en proposer un cantonnement (Titre II).

[172] Le terme *hégémonie* désigne la domination d'une puissance, d'un pays ou d'un groupe sur les autres, c'est-à-dire une domination sans partage, v. Dictionnaire Larousse, *Dictionnaire de français, V°* « Hégémonie ».

TITRE I – UNE NOTION EN EXPANSION

43. Un cumul de protections. La décennie de 1970 fut particulièrement prolifique pour le législateur français qui a reconnu plusieurs nouveaux droits aux individus. En 1970, le législateur a consacré, dans le code civil, un article à la protection de la vie privée[173]. Puis, en 1978, il a adopté une loi spéciale pour protéger les informations nominatives[174]. Dans le premier de ces textes, le législateur a été avare de précisions en affirmant un laconique « droit au respect de sa vie privée »[175]. L'œuvre de la jurisprudence a été particulièrement importante pour édifier les contours de cette notion et de son régime. Dans le deuxième texte, le législateur a été plus disert et a organisé les règles relatives aux traitements des informations nominatives par le secteur public et par le secteur privé[176]. Il a défini largement la notion d'information nominative comme « les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent »[177].

44. Le glissement sémantique. Malgré cette définition très large de la notion d'information nominative, le législateur français l'a remplacée par celle de donnée à caractère personnel à l'occasion de la transposition de la directive européenne de 1995[178]. Ce glissement sémantique n'est pas neutre et le législateur ne s'en cache pas. La notion de donnée à caractère personnel permet d'adopter une « neutralité technologique préservant la loi d'évolutions aujourd'hui imprévisibles »[179] et rend possible la prise en compte des nouvelles techniques d'identification[180].

---

[173] La loi nº 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens a renouvelé la rédaction de l'article 9 du code civil pour garantir le respect de la vie privée, *JORF* 19 juill. 1970, nº 0166, p. 6755.
[174] Loi nº 78-17 du 6 janv. 1978, relative à l'informatique, aux fichiers et aux libertés, *JORF* 7 janv. 1978, nº 6, p. 227.
[175] *Rép. civ.* Dalloz, *Vº* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), nº 42.
[176] Une dualité de régime était prévue par cette loi avec un régime beaucoup plus contraignant pour le secteur public que pour le secteur privé, v. *infra*, nº 305.
[177] Art. 4 de la loi nº 78-17 du 6 janv. 1978.
[178] C'est la loi nº 2004-801 du 6 août 2004 qui a transposé, en droit français, la directive CE nº 95/46.
[179] G. Gouzes, « Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », Assemblée nationale, nº 3526, 9 janv. 2002, p. 17 ; v. les termes similaires utilisés dans le rapport sénatorial, A. Türk, « Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », Sénat, nº 218, 19 mars 2003, p. 22.
[180] G. Braibant, « Données personnelles et société de l'information. Rapport au Premier ministre sur la transposition en droit français de la directive nº 95/46 », La Documentation française, 1998, p. 45.

45. Des termes technologiquement neutres. Les termes choisis pour composer la notion de donnée à caractère personnel favorisent une interprétation étendue de celle-ci. En effet, chacun de ces termes est celui – par rapport à ses synonymes – dont le champ d'application est le plus large. L'analyse de chacun de ces termes est importante pour comprendre l'étendue de la notion et ses éventuelles limites. Elle permet aussi de mieux appréhender l'usage des marges éventuelles d'interprétation.

46. L'utilisation des marges d'interprétation. Les termes composant la notion de donnée à caractère personnel offraient des possibilités d'interprétation larges. Celles-ci ont été utilisées pleinement par les acteurs de la protection des données[181]. Ces interprétations renforcent le sentiment que cette notion subit une extension irrésistible dont les limites s'affaissent progressivement au point qu'il est possible de se demander s'il existe aujourd'hui des données non personnelles.

47. Plan. L'étude des composantes de la notion de donnée à caractère personnel (Chapitre I) révèle un territoire fécond, propice à son essor (Chapitre II).

[181] Les acteurs de la protection des données à caractère personnel sont les autorités auxquelles revient un pouvoir d'agir dans le domaine des données à caractère personnel et incluent le législateur, le juge et les autorités de protection des données. Il pourrait être ajouté que les individus ou les associations, en tant qu'ils peuvent agir devant les tribunaux en défense des données à caractère personnel, font également partie des acteurs de la protection. À ce stade du développement, nous nous en tiendrons à une interprétation stricte des acteurs incluant seulement le législateur, le juge et les autorités de protection des données.

Chapitre I – Les composantes de la notion de donnée à caractère personnel

48. Définir les données à caractère personnel. Pour connaître le domaine du droit des données à caractère personnel, il convient au préalable de déterminer à quoi la donnée à caractère personnel renvoie. Une telle étude aide à circonscrire le champ de la protection des personnes qui ressort de cette matière. En effet, les données protégées sont celles qui entrent dans la notion de donnée à caractère personnel. Dès lors, l'étude de ses composantes est cruciale. La définition de la donnée à caractère personnel est fondée sur deux critères : les données à caractère personnel sont *des données* qui se *rapportent à une personne physique*[182].

49. Les données à caractère personnel sont *des données*. Puisque les données à caractère personnel sont des données, déterminer ce que recouvre la notion de « donnée » apparaît nécessaire. Or, tenter de la définir, c'est être confronté à une grande variété de significations : elle est si évasive que la plupart des essais de définitions juridiques ont échoué par excès de généralité[183].

50. Les données à caractère personnel sont des données *se rapportant à une personne physique*. Pour caractériser l'existence d'une donnée à caractère personnel, il faut établir un lien avec une personne physique. Cette dernière est une notion connue du droit civil. Pour autant, il n'est pas certain que la notion de personne physique en droit des données à caractère personnel se calque parfaitement sur celle du droit civil. De plus, le lien entre la donnée et la personne peut prendre plusieurs formes. Évidemment, les liens directs caractérisent immanquablement le rattachement nécessaire et déclenchent la qualification de donnée à caractère personnel. Qu'en est-il des liens potentiels et indirects ? Caractérisent-ils un rattachement suffisant ?

51. Plan. La notion de donnée à caractère personnel s'articule autour de deux critères de qualification qu'il convient d'étudier successivement : la notion de donnée (Section I) et le rattachement à une personne physique (Section II).

---

[182] Art. 4 § 1 du règlement UE nº 2016/679.
[183] V. not. P.-Y. Marot, *Les données et informations à caractère personnel. Essai sur la notion et ses fonctions,* th. Nancy, 2007, p. 66.

SECTION I – LA DONNÉE

52. Les notions proches. Pour analyser la notion de donnée, il faut d'abord la distinguer des termes qui lui sont proches : l'information, le document et le fichier. La notion de renseignement personnel, connue du droit canadien, aurait également pu offrir une mise en perspective intéressante[184]. Toutefois, celle-ci est souvent interprétée de manière similaire à celle de donnée à caractère personnel et trouve un écho limité en droit français et européen[185].

53. Plan. Plutôt que de tenter de définir la notion de donnée de manière positive, nous proposons de la mettre en perspective avec des notions voisines (§ I). Ces comparaisons montrent l'étendue de la notion de donnée. Cette dernière est si large que les auteurs se disputent la catégorie juridique à laquelle elle doit être rattachée (§ II).

§ I. La singularité de la notion de donnée

54. Plan. La comparaison de la notion de donnée avec d'autres notions similaires fait ressortir sa caractéristique principale : son adaptabilité. Dans un premier temps, la notion de donnée sera confrontée à celle d'information (A), puis à celle de fichier (B) et, enfin, à celle de document (C).

A. La donnée et l'information

55. L'omniprésence de l'information. L'information est devenue un sujet majeur. Elle inspire des travaux dans des domaines aussi éclectiques que la presse, l'informatique, la littérature, les mathématiques ou encore la philosophie. Elle envahit l'espace social, à tel point que l'on parle de l'avènement d'une « société de l'information »[186]. En dépit de cette place centrale et transversale, il est fréquent que le terme soit employé sans aucune sorte de précaution liminaire, comme si sa signification

---

[184] Pour un panorama relatif à la protection des données et de la vie privée au Canada, v. B. Pelletier, « La protection de la vie privée au Canada », *Revue juridique Thémis* 2001, vol. 35, p. 485 s. [35 RJT 485].
[185] V. Commissariat à la protection de la vie privée du Canada, « Renseignements personnels », oct. 2013.
[186] On entend par société de l'information « une société qui fait un usage intensif des réseaux d'information et de la technologie de l'information, produit de grandes quantités de biens et de services d'information et de communication et possède une industrie de contenus diversifiée », H. Jeskanen-Sundström, « ICT Statistics at the New Millennium. Developing Official Statistics. Measuring the Diffusion of ICT and its Impacts », *IAOS* 2001, Japon et S. T. Balima, « Une ou des "sociétés de l'information" ? », *Hermès La Revue* 2004, nº 40, p. 205, spéc. p. 206. Pour une approche critique de cette expression, v. M. Ménard, « Autoroutes de l'information et société de l'information : pour un renversement de perspective », in *Les autoroutes de l'information : enjeux et défis,* dir. J. Frémont et J.-P. Ducasse, Université de Montréal, 1996, p. 103 s.

allait de soi[187]. Pourtant sa définition demeure loin d'être consensuelle, l'information apparaît comme un terme général et abstrait, ayant tendance à désigner des réalités très variées[188].

56. La dualité de signification de l'information. Le terme information vient du latin *informatio* et vise l'action de former, de façonner, de donner forme à une matière[189]. À ce premier sens, plutôt objectif, du terme information s'en est progressivement ajouté un second, plus subjectif, lié à l'action de faire connaître quelque chose à quelqu'un[190]. Ce passage du sens objectif, qui décrit quelque chose de neutre, au sens subjectif se retrouve notamment dans les écrits de Descartes[191].

57. Les difficultés d'établir une définition juridique de la notion d'information. La polysémie du terme « information » se retrouve également en droit puisque l'information fait l'objet d'usages multiples qui renvoient à des problèmes juridiques distincts[192]. Le terme information transcende les domaines puisqu'il se retrouve notamment dans la matière pénale[193], civile[194] le droit des affaires[195], ou le droit administratif[196].

Selon Monsieur Jean-Christophe Galloux, lorsque la doctrine essaie de la définir, elle a tendance à se partager entre quatre attitudes : utilitariste, pragmatique, sceptique et prospective[197]. La première attitude doctrinale définit l'information selon

---

[187] S. Leleu-Merviel, *La traque informationnelle*, ISTE Éditions, 2017, p. 55.
[188] P.-Y. Marot, *Les données et informations à caractère personnel. Essai sur la notion et ses fonctions,* th. Nancy, 2007, p. 65.
[189] É. Littré, *Le nouveau Littré. Le dictionnaire de référence de la langue française*, Garnier, 2007, *V°* « Information ». D'ailleurs, selon la définition fournie par le dictionnaire Gaffiot, le terme est lié à l'idée, la conception, et signifie « la représentation d'une idée par l'image d'un mot » ou l'« explication d'un mot », F. Gaffiot, *Dictionnaire Latin-Français*, Hachette, 2000, *V°* « Infōrmātīō », sens 1.
[190] R. Capurro, « Past, present, and future of the concept of information », *Triple C* 2009, vol. 7, p. 125 s. [7 TRIPLE C 125], spéc. p. 129.
[191] R. Descartes, « Meditationes de prima philosophia. Secudae Responsines », in *Œuvres*, vol. VII, dir. C. Adam et P. Tannery, Vrin, 1996, p. 160.
[192] V. par ex., la variété des travaux au sein de l'étude *L'information en droit privé : travaux de la conférence d'agrégation*, dir. P. Lagarde et Y. Loussouarn, LGDJ, 1978.
[193] Notamment au travers des délits de divulgation de fausses informations prévus aux articles 322-14 et 411-10 du code pénal.
[194] Notamment avec l'article 16-8 du code civil qui fait référence aux informations permettant l'identification d'une personne physique, l'article 1137 relatif à la réticence dolosive ou l'article 1112-1 relatif à l'obligation d'information.
[195] Notamment avec l'article L. 151-1 du code de commerce qui protège certaines informations au titre du secret des affaires.
[196] Notamment avec l'article L. 321-1 du code des relations entre le public et l'administration qui sanctuarise le droit à la réutilisation des informations publiques.
[197] J.-C. Galloux, « Ébauche d'une définition juridique de l'information », *D.* 1994, p. 229, n° 8.

son contenu et non en fonction de sa nature[198]. La deuxième attitude doctrinale établit, quant à elle, une typologie des informations, en fonction de leur reconnaissance par le droit[199]. Ainsi, seules les informations susceptibles d'être qualifiées juridiquement comme telles entrent dans la notion. La troisième attitude consiste à douter de la possibilité même pour l'information de recevoir une définition juridique[200]. Enfin, la quatrième attitude présente l'information comme quelque chose de primaire et qui est protégé[201].

En dépit de ces difficultés, quelques auteurs ont tenté cet aventureux exercice[202]. Ainsi, Pierre Catala définit l'information très largement puisqu'il considère qu'elle « est d'abord expression, formulation destinée à rendre un message communicable ; elle est ensuite communiquée, ou peut l'être, à l'aide du signe choisi pour porter le message à autrui »[203]. La définition de Pierre Catala reprend donc le balancement entre le sens objectif et subjectif de la notion d'information. S'appuyant également sur cette dualité, Monsieur Pierre-Yves Marot définit l'information comme « un message, une représentation de faits ou d'idées ayant une signification et susceptible de communication »[204]. Ces deux définitions, bien qu'utiles en théorie, souffrent d'un trop haut degré de généralité, les rendant peu praticables[205]. Pour Monsieur Jean-Christophe Galloux, l'information serait plutôt « la forme ou l'état particulier de la matière ou de l'énergie susceptible d'une signification »[206]. Pourtant, l'information n'est ni énergie, ni matière ; elle n'a aucune réalité physique en dehors de son support[207]. Aucune de ces

---

[198] J.-M. Mousseron, J. Raynard et T. Revet, « De la propriété comme modèle », in *Mélanges A. Colomer*, Litec, 1993, p. 281 s., n° 14, spéc. p. 286. Pour une critique de cette définition, v. P. Catala, « Ébauche d'une théorie juridique de l'information », *D.* 1984, p. 97, n° 3.

[199] J.-M. Auby et R. Ducos-Ader, *Le droit de l'information*, Dalloz, 1982, n° 1, p. 1 s.

[200] V. not. A. Lucas, *Le droit de l'informatique*, PUF, 1987, n° 304, p. 353.

[201] Par exemple, pour Monsieur Pierre Leclercq, « l'information est quelque chose de primaire qui, souvent, a une valeur plus par l'exclusivité de sa source que par sa nature, et qui est protégée soit dans son environnement, son circuit de diffusion, soit comme élément de la personne, soit, rarement, comme élément de patrimoine », v. P. Leclercq, « Essai sur le statut juridique des informations », in *Les flux transfrontières de données : vers une économie informationnelle*, dir. A. Madec, La Documentation française, 1982, p. 122.

[202] Pour une histoire des propositions de définitions de l'information, v. E. Daragon, « Étude sur le statut juridique de l'information », *D.* 1998, p. 63, n^{os} 10 s.

[203] P. Catala, « Ébauche d'une théorie juridique de l'information », *D.* 1984, p. 97, n° 5 ; P. Catala, « La "propriété" de l'information », in *Mélanges P. Raynaud*, Dalloz, 1985, p. 97 s., n° 6, spéc. p. 99. Cette définition se rapproche de celle formulée par l'arrêté portant enrichissement du vocabulaire de l'informatique selon lequel l'information est « un élément de connaissance susceptible d'être représenté à l'aide de conventions pour être conservé, traité ou communiqué », v. arrêté du 22 déc. 1981, *JORF* 17 janv. 1982, n° 14 numéro complémentaire, p. 624.

[204] P.-Y. Marot, *Les données et informations à caractère personnel. Essai sur la notion et ses fonctions,* th. Nancy, 2007, p. 66.

[205] J.-C. Galloux, « Ébauche d'une définition juridique de l'information », *D.* 1994, p. 229, n° 12.

[206] J.-C. Galloux, « Ébauche d'une définition juridique de l'information », *D.* 1994, p. 229, n° 25.

[207] E. Daragon, « Étude sur le statut juridique de l'information », *D.* 1998, p. 63, n^{os} 12 s. Madame Elise Daragon propose sa propre définition de l'information, entendue comme « un message porteur de signification dont la valeur patrimoniale est fonction de sa densité informative ». V. aussi, obs. H. Croze ss Cass. crim., 29 avr. 1986, *JCP G* 1987, chron. 20788, n° 13.

définitions n'emporte donc une adhésion parfaite. Elles illustrent plutôt la polysémie du terme d'information et sa difficile appréhension par le droit.

58. Discussions sur les liens entre la notion d'information et celle de donnée. Après avoir tenté, non sans difficulté et sans véritable succès, de définir la notion d'information, il est intéressant d'étudier les rapports que cette notion entretient avec celle de donnée. Prise dans son sens étymologique, la notion de donnée désigne ce qui est à la base d'un raisonnement, ce à partir de quoi une décision ou une action est prise[208]. Dans le langage courant, la donnée fait référence à un fait ou un principe indiscuté : elle est ce qui est connu immédiatement[209]. La donnée s'oppose donc au résultat du raisonnement tenu, du processus décisionnel qui est l'information produite, laquelle pourra ensuite être communiquée. La donnée *précède* l'information, qui fait figure de produit fini ; elle en est la matière première[210].

Lorsque Claude Shannon, le père fondateur de la théorie de l'information, s'est intéressé aux modalités de sa transmission, il est parti de ce postulat et a montré comment minimiser la quantité de données représentant une information[211]. Cette théorie a trouvé un écho particulier dans les écrits de Pierre Catala, qui considérait que si l'essence de l'information est d'être communicable, sa nature est d'être communiquée[212]. L'information est donc le fruit d'une activité humaine prenant la forme d'un message visant à être communiqué[213]. La donnée serait, quant à elle, un élément brut.

Pour Madame Frédérique Lesaulnier au contraire, la donnée serait une information valorisée[214]. La donnée aurait une valeur ajoutée technologique issue du formatage et de la saisie sur un support informatique permettant l'exploitation de l'information[215]. Cette analyse, fondée sur l'apport du formatage et de la saisie, semble

---

[208] *Dictionnaire de l'Académie française*, 9e éd., *Vo* « Donnée », sens 1.
[209] *Dictionnaire de l'Académie française*, 9e éd., *Vo* « Donnée », sens 1 et 2.
[210] Le Robert définit notamment la donnée comme « ce qui est admis, connu ou reconnu, et qui sert de base à un raisonnement, de point de départ pour une recherche », v. A. Rey et J. Rey-Debove, *Le petit Robert de la langue française*, 2017, Le Robert, *Vo* « Donnée », sens 2.
[211] C. Shannon, « A mathematical theory of communication », *The Bell System Technical Journal* 1948, vol. 27, p. 379.
[212] P. Catala, « Ébauche d'une théorie juridique de l'information », *D.* 1984, p. 97, no 5.
[213] P. Catala, « Ébauche d'une théorie juridique de l'information », *D.* 1984, p. 97, no 9. La distinction n'est pas explicitement effectuée entre les deux notions. D'ailleurs Pierre Catala a tendance à utiliser les deux termes de manière interchangeable. Pour autant, face aux évolutions des technologies, une telle interprétation des écrits de Pierre Catala semble parfaitement possible.
[214] F. Lesaulnier, *L'information nominative,* th. Paris II, 2005, no 16, p. 30.
[215] F. Lesaulnier, *L'information nominative,* th. Paris II, 2005, no 16, p. 30. « Une donnée se distingue d'une information par la transformation que cette dernière subit pour être utilisée en vue d'un traitement informatique. Selon cette acception, la donnée est une information valorisée, qui possède une valeur ajoutée d'ordre

assez éloignée de la réalité des traitements actuels de l'information. En effet, si pendant longtemps les données saisies et enregistrées par une personne était le principal objet des traitements effectués par les ordinateurs, cela n'est plus le cas. Le nombre de capteurs et de données générées par défaut, sans saisie active de l'utilisateur, a explosé. Ainsi, la plupart des données sont désormais générées par défaut *via* le support informatique. À ce facteur s'ajoutent également les progrès fulgurants des ordinateurs dans l'interprétation des données ayant des formatages moins structurés[216].

Plutôt que de montrer une imperméabilité entre les deux termes, ces analyses illustrent surtout leurs liens et leurs rapports. En l'état de ces constatations, il faut bien reconnaître que les deux notions sont très proches et que, sur le plan juridique, la distinction entre elles n'entraîne pas toujours des conséquences. D'ailleurs, Monsieur Pierre-Yves Marot remarquait que « les interactions entre les deux notions semblent trop étroites pour justifier une distinction solide »[217].

59. La donnée, source de l'information. Aujourd'hui, la donnée semble être une matière première de la production d'informations, et les informations sont des données traitées de manière à avoir un sens pour la personne qui les reçoit. D'ailleurs, selon Mesdames Alexandra Bensamoun et Celia Zolynski, l'expression *big data* évoque « la constitution et l'exploitation de grandes masses de données dans le but de les transformer en information »[218]. Une telle définition illustre bien le mouvement de transformation de la donnée, laquelle précède l'information. Dès lors, il semble que toute information contient nécessairement une donnée, mais sa réciproque ne se vérifie pas toujours.

En définitive, la notion de donnée s'inscrit dans une sémantique en rapport avec l'informatique et les mathématiques et apparaît plus neutre que celle d'information, laquelle a tendance à faire référence à l'opération effectuée sur une donnée. Cette

technologique », v. I. de Lamberterie et J.-H. Lucas (dir.), *Informatique, libertés et recherche médicale*, CNRS, 2001, nº 157 citant l'arrêté du 22 déc. 1981, *JORF* 17 janv. 1982, nº 14 numéro complémentaire, p. 624.

[216] V. not. le projet de Google « Cloud Natural language » qui illustre les capacités des ordinateurs d'interpréter du texte non structuré.

[217] P.-Y. Marot, *Les données et informations à caractère personnel. Essai sur la notion et ses fonctions,* th. Nancy, 2007, p. 70. Madame Jessica Eynard, dans sa thèse sur les données personnelles, rejoint ce point de vue en considérant que « ces deux termes sont, en général et par commodité, utilisés comme des synonymes. Tel est aussi le parti pris tout au long de ce travail », v. J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 17. V. également, I. de Lamberterie et J.-H. Lucas (dir.), *Informatique, libertés et recherche médicale*, CNRS, 2001, nº 157.

[218] A. Bensamoun et C. Zolynski, « *Big data* et *privacy* : comment concilier nouveaux modèles d'affaires et droits des utilisateurs ? », colloque *Transformations sociales et ère numérique* du Forum mondial des sciences sociales, Montréal, 15 oct. 2013, *LPA* 18 août 2014, nº 164, p. 8, § 1.

distinction illustre le caractère particulièrement accueillant de la notion de donnée. Pour autant, sur le plan juridique, il est fréquent que ces notions soient utilisées de manière équivalente et il apparaît que toute distinction trop stricte ne peut prospérer. Dans notre étude, nous tâcherons d'avoir recours à la notion de donnée chaque fois que le contexte de l'informatique est incontestable.

B. La donnée et le fichier

60. La définition du fichier. Le terme fichier est dérivé du mot fiche. Étymologiquement, le fichier est un « ensemble de fiches » ou un « meuble où l'on range les fiches »[219]. Le dictionnaire de l'Académie française définit la fiche comme la « feuille de papier rigide ou de carton souple, d'un format réduit, sur laquelle on porte des renseignements et qu'on classe avec d'autres pour constituer un ensemble de données »[220]. Ainsi, le fichier est intrinsèquement lié à l'idée de structuration de données.

61. L'histoire européenne et les fichiers. La notion de fichier a plutôt mauvaise réputation : depuis l'affaire des fiches du début du XX^e^ siècle[221] jusqu'au récent fichier « Titres électroniques sécurisés » (dit « TES »)[222], en passant par le « fichier juif » élaboré pendant la Seconde Guerre mondiale[223], le fichier éveille les suspicions. D'ailleurs, le terme « fichier » est souvent associé aux régimes totalitaires, notamment au régime nazi qui avait élaboré des fichiers ciblant certaines minorités ou certains types de populations[224], qui ont facilité et accéléré les atrocités perpétrées pendant la Seconde Guerre mondiale[225].

---

[219] É. Littré, *Le nouveau Littré. Le dictionnaire de référence de la langue française*, Garnier, 2007, *V°* « Fichier ». En informatique, la notion de fichier renvoie à un stockage d'informations qui prend la forme d'un ensemble de données structurées, v. CNIL, *Les définitions*, *V°* « Fichier ».

[220] *Dictionnaire de l'Académie française*, 9^e^ éd., *V°* « Fiche », sens III.

[221] G. Thuillier, « Autour d'Anatole France : le capitaine Mollin et l'affaire des fiches en 1904 », *Revue administrative* 1986, n° 234, p. 549 ; « À propos de l'affaire des fiches. Les mésaventures du préfet Gaston Joliet », *Revue administrative* 1994, n° 278, p. 133 ; « À propos de l'affaire des fiches : le maintien du système des fiches de 1905 à 1914 », *Revue administrative* 1997, n° 295, p. 21.

[222] Ce fichier a été instauré par le décret n° 2016-1460 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité, *JORF* 30 oct. 2016, n° 0254, texte 18, v. not. R. Perray, « Le fichier TES : un réel danger ? », *D.* 2017, p. 56 ; G. Koubi, « Le fichier des "titres électroniques sécurisés" entériné », *JCP adm.* 2016, n° 47, p. 2300.

[223] Les Juifs étaient tenus de se déclarer comme tel depuis l'ordonnance du 27 septembre 1940 relative aux mesures contre les Juifs, *JO des ordonnances du Gouverneur militaire pour les territoires français occupés* du 26 janvier 1941, p. 19.

[224] P.-H. Prélot, *Droit des libertés fondamentales*, 2^e^ éd., Hachette Supérieur, 2010, n° 462, p. 188.

[225] Pour introduire ses développements sur le droit des données personnelles, René Rémond rappelait la sensibilité particulière des fichiers élaborés pendant la Seconde Guerre mondiale : « La mémoire douloureuse du fichage des Juifs et de l'obligation du port de l'étoile jaune, préludes à la déportation massive, ont longtemps fait peser en

La défiance des Français à l'égard de la création des fichiers s'inscrit donc une histoire ancienne[226]. D'ailleurs, la loi Informatique et libertés en est une preuve supplémentaire puisque cette loi a justement été adoptée en réponse au scandale du fichier « SAFARI »[227].

62. Relations entre la notion de fichier et celle de donnée. La loi Informatique et libertés n'avait pas défini la notion de fichier et employait le terme uniquement à l'article 45 pour étendre, par ricochet, certaines de ses obligations aux fichiers non informatisés ou mécanographiques. En l'absence de définition légale, la notion de fichier était incertaine et son interprétation a fait l'objet de désaccords entre la chambre criminelle de la Cour de cassation et la CNIL[228]. Grâce à l'adoption de la directive européenne en 1995, ces incertitudes se sont dissipées, et le règlement européen a confirmé qu'un fichier est « tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique »[229]. La définition retenue permet donc une interprétation large de la notion et montre le lien fort qu'elle entretient avec celle de donnée.

63. La donnée composante des fichiers. L'élément central de la notion de fichier repose sur l'idée de structuration des données ; c'est parce que les données sont organisées qu'elles deviennent accessibles[230]. Pour constituer un fichier, un ensemble de données doit lui préexister. La donnée apparaît donc comme une composante d'un

---

France, après 1945, une méfiance extrême à l'encontre de tout procédé permettant la conservation de renseignements personnalisés », R. Rémond, *Le « fichier juif »* (rapport au Premier ministre), Plon, 1996, p. 184.

[226] C'est sans doute ce qui explique l'émoi suscité en 2018 suite à la publication des travaux de l'organisation EU Disinfo Lab. Celle-ci avait élaboré une étude des comptes Twitter particulièrement actifs lors de « l'affaire Benalla » (du nom de l'ancien collaborateur de l'Élysée, Monsieur Alexandre Benalla). L'organisation avait remarqué un volume exceptionnel de tweets échangés sur le sujet, près de 4,5 millions de messages en français. Elle a alors cherché à savoir si cela était le reflet d'une éventuelle ingérence étrangère. L'étude avait constitué des fichiers de noms associés à de présupposées affiliations politiques. Après la consternation de l'opinion publique, la CNIL avait été saisie de nombreuses plaintes et leur instruction est actuellement effectuée en coordination avec son homologue belge. V. not. P. Januel, « L'affaire Benalla enflamme le Parlement », *Dalloz actualité* 20 juill. 2018.

[227] Ce scandale était né des révélations liées à la création d'un système centralisé – dénommé SAFARI – utilisant un numéro d'identification unique pour accéder aux centaines de fichiers publics. Pour plus de détails, v. *infra*, nº 174.

[228] Pour une analyse détaillée de ces divergences, v. J. Frayssinet, « La Cour de cassation et la loi informatique, fichiers et libertés, ou comment amputer une loi tout en raffermissant son application », *JCP G* 1988, I, p. 3323. Pour les problèmes engendrés par ces différences d'interprétation, v. *infra,* nº 527.

[229] Art. 4 § 6 du règlement UE nº 2016/679. Pour une interprétation de la notion de fichier par la Cour de justice de l'Union européenne, v. CJUE, 10 juill.2018, *Tietosuojavaltuutettu*, C-25/17, § 55 ; CJUE, 1 oct. 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände* c. *Planet49 GmbH,* C-673/17, § 52 s.

[230] *Le Lamy droit du numérique*, *Vº* « Historique de la notion de fichier », § 427, actu. 2020, dir. M. Vivant.

fichier : sans données, il n'est pas de fichier. Ainsi, la notion de fichier entretient un rapport de dépendance avec celle de donnée, quoique toute assimilation soit exclue. Ici encore, la notion de donnée apparaît technologiquement plus neutre que celle de fichier et semble plus générique.

C. La donnée et le document

64. La nature et les fonctions du document. Avant tout, le document est support : c'est un objet porteur d'informations. Vecteur matériel d'une information, il est défini par Paul Otlet comme « le moyen de transmettre des données informatives à la connaissance des intéressés »[231]. D'ailleurs, le terme document vient du latin *documentum* et *docere* qui signifie instruire, enseigner[232]. Le document permet donc aux humains d'échanger, de communiquer des informations à une ou plusieurs personnes, qu'elles soient ou non réunies physiquement. Par ailleurs, le document est aussi une assistance à la mémoire. Cette dualité fonctionnelle du document (naviguant entre communication et mémoire) existe depuis l'invention de la sculpture, de la gravure ou de l'écriture[233].

65. La définition juridique du document. Au sens juridique, la notion de document fait référence au *support* d'information[234]. Lors de l'adoption de la loi relative à l'accès aux documents administratifs[235], le législateur français avait privilégié le terme « document » à celui d'information, pourtant consacré quelques mois plus tôt dans la loi Informatique et libertés. Une telle préférence permettait de poser un principe simple : seules les informations ayant un support matériel peuvent être communiquées[236]. En l'absence de ce support, l'information publique ne pourra pas être transmise. La définition retenue par la loi de la notion de « document administratif » est très large puisque sont considérés comme tels, et ce, « quels que soient leur date, leur lieu de conservation, leur forme et leur support, les documents

---

[231] P. Otlet, *Traité de documentation*, Mundaneum, 1934, n° 141, p. 25.
[232] F. Gaffiot, *Dictionnaire Latin-Français*, Hachette, 2000, *V°* « dŏcĕō », sens I.
[233] A. Tricot, G. Sahut et J. Lemarié, *Le document : communication et mémoire*, De Boeck, 2016, p. 11.
[234] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *V°* « Document », sens 1, 2 et 3. Pour une analyse des définitions du document, v. F. Labarthe, *La notion de document contractuel,* th. Paris I, 1994, LGDJ, n° 2, p. 2.
[235] Loi n° 78-753 du 17 juill. 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal, *JORF* 18 juill. 1978, n° 166, p. 2851, désormais codifiée aux articles L. 300-1 s. du code des relations entre le public et l'administration.
[236] *Rép. cont. adm.* Dalloz, *V°* « Communication des documents administratifs », par A. Lallet et P. Nguyen Duy, 2019, nos 53 s.

produits ou reçus, dans le cadre de leur mission de service public, par l'État, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission »[237]. La notion de document se retrouve également dans d'autres domaines juridiques, notamment en droit commercial avec le crédit documentaire[238], ou en droit des transports avec les documents de transport[239]. Dans ces domaines aussi, la notion de document fait plutôt référence à la matérialité de l'information plutôt qu'à son contenu.

66. Relations entre la notion de document et celle de donnée. Le terme document a trait au *contenant* alors que celui de donnée est apparenté au *contenu*. Le document a une fonction précise et définie à l'avance : il sert à la communication et à la conservation de données[240]. Quant à la donnée, sa fonction est moins spécifiée puisqu'elle enserre en son sein une vaste réalité d'éléments : de la lettre au signe, en passant par le chiffre[241]. Ainsi, tout document contient nécessairement des données, au risque sinon d'être une page entièrement blanche. Ici encore la réciproque ne se vérifie pas puisque des données existent même sans support matériel. Ainsi, si les deux termes sont liés, la notion de donnée apparaît plus neutre et moins enfermée dans une fonction précise et définie à l'avance. Elle est façonnable au gré des évolutions technologiques et conserve une neutralité qui encourage son essor.

La neutralité de la notion de donnée se retrouve dans la variété des qualifications juridiques qu'elle reçoit.

---

[237] Art. L. 300-2 du code des relations entre le public et l'administration.
[238] Le crédit documentaire est « un instrument de règlement, par l'intermédiaire d'un établissement de crédit (banque), du prix de prestations commerciales. Un acheteur obtient de l'émetteur du crédit l'engagement de régler à son fournisseur, contre production de certains documents justificatifs, le prix d'une prestation commerciale », v. *Rép. com.* Dalloz, *V°* « Crédit documentaire », par J. Stoufflet, 2004 (actu. 2015), n° 1.
[239] « Pour établir le document de transport, le donneur d'ordre doit fournir au transporteur diverses informations qui varient selon le contrat type applicable : les dates de prise d'effet et de fin de contrat (contrat type à temps), - les noms et adresses de l'expéditeur et du destinataire (..) - les caractéristiques des installations de chargement et de déchargement (…), - la date de mise à quai et celle d'arrivée à destination (…), - la nature de la marchandise, son poids, son volume et/ou ses dimensions, son caractère dangereux ou périssable, les précautions à prendre pour son transport (…) - le prix du transport et le débiteur du fret (…). Le document de transport matérialisant l'accord des parties est établi sur la base de ces indications fournies par écrit ou par tout autre procédé permettant leur mémorisation (contrats types) », *Rép. com.* Dalloz, *V°* « Transports fluviaux », par V. Bailly-Hascoët, 2003 (actu. 2015), n° 41.
[240] A. Tricot, G. Sahut et J. Lemarié, *Le document : communication et mémoire,* De Boeck, 2016, p. 19 s.
[241] Suzanne Briet a mené d'importants travaux relatifs à la qualification des documents et s'interrogeait sur les limites à cette notion : « Une étoile est-elle un document ? Un galet roulé par un torrent est-il un document ? Un animal vivant est-il un document ? Non. Mais sont des documents les photographies et les catalogues d'étoiles, les pierres d'un musée de minéralogie, les animaux catalogués et exposés dans un zoo », S. Briet, *Qu'est-ce que la documentation ?*, EDIT, 1951, p. 7.

§ II. La pluralité des qualifications potentielles de la donnée

67. La difficulté de qualifier abstraitement la donnée. Lorsque les auteurs ont tenté de définir la donnée, ils ont régulièrement cherché à l'assimiler à des catégories juridiques connues. Dans ce travail de classification, inhérent au droit[242], les auteurs se sont souvent inspirés des travaux doctrinaux relatifs à l'information. En effet, ces notions étant très proches, d'intéressants parallèles peuvent être dressés.

En matière de qualification de l'information, deux courants doctrinaux s'opposent[243]. D'un côté, certains auteurs affirment son caractère patrimonial : celle-ci serait un bien[244], ou du moins, une chose susceptible d'appropriation[245]. De l'autre, les auteurs écartent cette idée en considérant que la propriété de l'information serait une « éternelle chimère »[246], voire un malentendu[247]. Ces thèses ont été amplement reprises à l'occasion des débats relatifs à la qualification des données, particulièrement en ce qui concerne les données à caractère personnel. Sans vouloir analyser l'ensemble des arguments propres à chacune de ces théories, notre propos visera simplement à montrer la tendance qui ressort de cette diversité de qualifications : la donnée est un immense réceptacle permettant des qualifications opposées.

68. Plan. L'opposition entre les doctrines patrimoniales (A) et personnalistes (B) témoigne du caractère foisonnant de la notion de donnée (C).

A. Les doctrines patrimoniales

69. Des questions anciennes. D'apparence nouvelle, la question du caractère patrimonial de la donnée s'inscrit en réalité dans un travail de qualification ancien. En effet, la doctrine s'interroge depuis plusieurs décennies sur le caractère patrimonial ou extrapatrimonial de l'information, et les liens existant entre ces notions permettent

---

[242] Pour Madame Muriel Fabre-Magnan, « la qualification est une opération essentielle du droit : elle consiste à faire entrer un fait ou un ensemble de faits dans une catégorie juridique afin de déclencher l'application du régime correspondant. (…) il n'est donc pas possible de faire du droit sans faire des distinctions », M. Fabre-Magnan, *Introduction au droit,* PUF, 2018, p. 76. Pour Gérard Cornu, la qualification juridique, « est l'une des plus fondamentales de la science juridique », G. Cornu, *Droit civil. Introduction. Les personnes. Les biens*. 11e éd., Montchrestien, 2003, nº 194, p. 87. Pour une analyse critique du conceptualisme juridique, v. P.-E. Audit, *La naissance des créances : approche critique du conceptualisme juridique*, th. Paris II, 2013, Dalloz.

[243] Pour une brève présentation de ces courants, v. par ex. V.-L. Benabou et J. Rochfeld, *À qui profite le clic ? Le partage de la valeur à l'ère numérique*, Odile Jacob, 2015, p. 52 s.

[244] P. Catala, « Ébauche d'une théorie juridique de l'information », *D.* 1984, p. 97, nº 3.

[245] J.-C. Galloux, « Ébauche d'une définition juridique de l'information », *D.* 1994, p. 229, nº 26.

[246] N. Mallet-Poujol, « Appropriation de l'information : l'éternelle chimère », *D.* 1997, p. 330.

[247] J. Passa, « La propriété de l'information, un malentendu ? », *Dr. et Pat.* 2001, nº 91, p. 65.

d'importants rapprochements. Le développement de la « société de données » n'a fait qu'amplifier ces interrogations et les étendre à la qualification de donnée.

70. L'information comme un bien. Pierre Catala, précurseur en la matière, a établi en 1984 une typologie de l'information reposant sur le postulat selon lequel l'information serait un *bien,* susceptible d'appropriation[248]. Dans son sens le plus ordinaire, le bien désigne toute réalité matérielle appartenant à quelqu'un[249]. Aborder la définition de bien invite donc à s'intéresser au rapport que celui-ci entretient avec la personne[250]. Il s'agit d'abord d'un rapport d'*opposition* : les biens sont l'autre des personnes, ce qui pour elles constituent le monde extérieur[251]. D'ailleurs, le droit établit de longue date une distinction rigoureuse entre le patrimoine[252], projection de la personne dans le domaine pécuniaire, et la personne elle-même qui plane au-dessus des intérêts matériels[253]. Ensuite, c'est un rapport de *sujétion* : les biens servent les personnes, ils appartiennent à leur usage et permettent de satisfaire leurs besoins[254]. Enfin, c'est un rapport d'*utilité* qui lie le bien à la personne : ils sont objets de désirs pouvant être satisfaits.

La typologie élaborée par Pierre Catala classe les informations en fonction de leur *rapport à la personne*[255]. Celles rattachées à la personne le seraient soit par un lien

---

[248] P. Catala, « Ébauche d'une théorie juridique de l'information », *D.* 1984, p. 97, n° 3. La qualification de l'information comme un bien a été reprise par plusieurs auteurs, notamment Monsieur Michel Vivant, selon qui « toutes les propriétés intellectuelles que connaît notre droit reposent sur la reconnaissance du bien-information », M. Vivant, « À propos des "biens informationnels" », *JCP G* 1984, I, p. 3132.

[249] *Dictionnaire de l'Académie française*, 9e éd., *V°* « Bien », sens II.1. La notion de bien fait l'objet de nombreuses discussions en droit français, v. par ex. C. Grzegorczyk, « Le concept de bien juridique : l'impossible définition ? », in *Les biens et les choses, Archives de Philosophie du Droit* 1979, t. 24, Sirey, p. 258.

[250] Le Vocabulaire juridique de l'Association Capitant définit les biens selon leur rapport avec une personne puisque ce sont « tous les éléments mobiliers ou immobiliers qui composent son patrimoine, à savoir les choses matérielles (biens corporels) qui lui appartiennent et les droits (autres que la propriété) dont elle est titulaire (biens incorporels) », v. G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *V°* « Bien », sens 2.

[251] *Rép. civ.* Dalloz, *V°* « Biens », par R. Libchaber, 2016 (actu. 2019), nos 5 s.

[252] En l'absence de définition du patrimoine dans le code civil, c'est la doctrine qui s'est chargée de le définir. Si la notion a fait l'objet d'importants travaux doctrinaux, la construction d'Aubry et Rau, de la seconde moitié du XIXe siècle, reste fondatrice. Selon eux, le patrimoine est l'ensemble des rapports de droit appréciables en argent, qui ont pour sujet actif ou passif une même personne et qui sont envisagés comme formant une universalité juridique, v. C. Aubry et C. Rau, *Cours de droit civil français d'après la méthode de Zachariæ,* t. 9, 5e éd., par E. Bartin, Librairies techniques, 1917, n° 574, p. 333 s. Sur la notion juridique de patrimoine, v. A. Sériaux, « La notion juridique de patrimoine », *RTD civ.* 1994, p. 801.

[253] L. Josserand, « La personne humaine dans le commerce juridique », *D.* 1932, chron. 1. V. aussi, A. Jack, « Les conventions relatives à la personne physique », *Revue critique de législation et de jurisprudence* 1933, p. 362, spéc. p. 369.

[254] F. Terré et P. Simler, *Droit civil. Les biens*, 10e éd., Dalloz, 2018, n° 29, p. 37 s.

[255] V. déjà en ce sens, J. Audier, *Les droits patrimoniaux à caractère personnel*, th. Marseille, 1979, LGDJ.

d'attribution[256], soit par un lien de création[257]. Quant aux informations étrangères aux personnes, elles seraient une sorte de *res communis,* circulant librement et offerte à l'observation de tous[258]. Ainsi, selon cette conception, toute information attachée à la personne est appropriable car sa vocation naturelle est de posséder, sauf exception, une valeur patrimoniale[259]. Mais pour qu'une valeur devienne un bien, au sens juridique du terme, il faut que la société réponde, par le droit, aux soucis complémentaires de *réservation* et de *commercialisation* de son maître du moment[260]. En d'autres termes, le droit doit confier au titulaire le pouvoir de réserver cette valeur et, éventuellement, de la commercialiser[261]. Le titulaire bénéficierait d'un pouvoir d'interdiction exclusif et absolu à l'égard de l'information[262]. Certains auteurs contestent cette qualification et considère plutôt l'information comme une chose.

71. L'information comme une chose. Selon Monsieur Jean-Christophe Galloux, « alors que la plupart des auteurs qui ont tenté de définir la notion d'information ont déjà fait d'elle un bien, il serait plus juste d'affirmer qu'elle est d'abord une chose »[263]. Pour comprendre cette critique, il convient de distinguer ces deux notions. Lorsque la doctrine a tenté de définir la notion de bien, elle l'a d'abord articulée avec celle de chose. Pour passer de la chose au bien, le droit de propriété demeure le modèle le plus cité[264]. L'article 544 du code civil définit la propriété comme « le droit de jouir et disposer des choses de la manière la plus absolue, pourvu qu'on n'en fasse pas un usage prohibé par les lois ou par les règlements ». Ainsi, le passage de la chose au bien se

---

[256] L'attribution peut être directe, comme c'est le cas pour l'information nominative, ou indirecte, comme c'est le cas de l'article de presse par exemple, v. P. Catala, « Ébauche d'une théorie juridique de l'information », *D.* 1984, p. 97, n^os^ 12 s.

[257] La création est soit intellectuelle, soit industrielle, P. Catala, « Ébauche d'une théorie juridique de l'information », *D.* 1984, p. 97, n^o^ 13.

[258] P. Catala, « Ébauche d'une théorie juridique de l'information », *D.* 1984, p. 97, n^o^ 14. Sur la qualification de « commun » pour l'information, v. J. Rochfeld, *Les grandes notions du droit privé,* 2^e^ éd., PUF, 2013, *V^o^* « Le bien », n^o^ 17, p. 233. Pour une analyse de l'information comme bien commun, v. M. Cornu, F. Orsi et J. Rochfeld (dir.), *Dictionnaire des biens communs*, PUF, 2017, *V^o^* « Information (approche juridique) » ; M.-A. Chardeau, *Les choses communes*, th. Paris I, 2004, LGDJ, n^os^ 129 s., p. 154 s. et n^os^ 342 s., p. 365 s.

[259] La conception selon laquelle le bien renvoie à un aspect économique s'est développée dans les écrits du doyen Savatier. Celui-ci a associé le bien à tout ce qui était susceptible de représenter une utilité, v. R. Savatier, « Vers de nouveaux aspects de la conception et de la classification juridique des biens corporels », *RTD civ.* 1958, p. 1.

[260] J.-M. Mousseron, J. Raynard et T. Revet, « De la propriété comme modèle », in *Mélanges A. Colomer*, Litec, 1993, p. 281 s., n^o^ 13, spéc. p. 285. Sur le bien comme valeur réservée, v. J. Rochfeld, *Les grandes notions du droit privé,* 2^e^ éd., PUF, 2013, *V^o^* « Le bien », n^os^ 12 s., p. 223 s.

[261] J. Rochfeld, *Les grandes notions du droit privé,* 2^e^ éd., PUF, 2013, *V^o^* « Le bien », n^o^ 14, p. 228.

[262] J.-M. Mousseron, J. Raynard et T. Revet, « De la propriété comme modèle », in *Mélanges A. Colomer*, Litec, 1993, p. 281 s., n^o^ 16, spéc. p. 287. V. aussi pour une analyse de la protection du secret des correspondances par la propriété, V. Peltier, *Le secret des correspondances,* th. Aix-Marseille, 1998, PUAM, n^os^ 384 s., p. 211 s.

[263] J.-C. Galloux, « Ébauche d'une définition juridique de l'information », *D.* 1994, p. 229, n^o^ 26.

[264] Sur la propriété comme modèle, v. J.-M. Mousseron, J. Raynard et T. Revet, « De la propriété comme modèle », in *Mélanges A. Colomer*, Litec, 1993, p. 281 s., n^o^ 13, spéc. p. 285.

ferait par l'appropriation de celle-ci par une personne[265]. Mais pour Monsieur Frédéric Zenati, pour qu'une chose devienne un bien, il faut « que l'on envisage l'utilité de l'appréhender exclusivement afin de pouvoir en disposer »[266]. Un tel pouvoir d'interdire, exclusif et absolu, est propre au droit de propriété[267]. Appliquée à l'information, la propriété impliquerait donc la possibilité d'interdire à autrui son utilisation, c'est-à-dire d'interdire de la connaître et de l'exploiter[268]. Or, pour Monsieur Jean-Christophe Galloux, un tel pouvoir est inconcevable : l'information n'est pas appropriable en raison de sa nature dès lors que « l'homme a autant besoin d'informations que d'air ou d'eau »[269]. Par ailleurs, comment reconnaître ce pouvoir d'appropriation et d'exclusion lorsque rien n'empêche un tiers de découvrir l'information par lui-même[270] ?

72. Critiques des théories patrimoniales de l'information. Ces propositions doctrinales font l'objet de critiques, notamment parce que la reconnaissance d'un droit de propriété sur l'information aurait d'importantes conséquences négatives sur les libertés individuelles et la cohérence du droit[271]. Par exemple, pour Monsieur Jérôme Passa, reconnaître un droit de propriété sur l'information retire tout intérêt aux autres droits privatifs existants, tels que les brevets ou le droit d'auteur[272]. En effet, ces droits sont conçus de façon à atteindre un équilibre entre les intérêts particuliers (des

---

[265] J.-C. Galloux, « Ébauche d'une définition juridique de l'information », *D.* 1994, p. 229, n° 29. Cette conception selon laquelle une chose devient un bien par l'appropriation d'une personne est la conception doctrinale dominante, v. J. Rochfeld, *Les grandes notions du droit privé,* 2e éd., PUF, 2013, *V°* « Le bien », n° 5, p. 214.

[266] F. Zenati, *Essai sur la nature juridique de la propriété : contribution à la théorie du droit subjectif*, th. Lyon III, 1981, t. 2, n° 571, p. 786 s.

[267] C. Atias, *Droit civil. Les biens,* 12e éd., LexisNexis, 2014, n° 114, p. 88 s. ; F. Terré et P. Simler, *Droit civil. Les biens*, 10e éd., Dalloz, 2018, nos 142 s., p. 147 s.

[268] H. Croze, obs. ss Cass. crim., 29 avr. 1986, *JCP G* 1987, chron. 20788, n° 13.

[269] Selon Monsieur Jean-Christophe Galloux, « L'homme, à l'instar de tout être biologique, fonctionne comme un système ouvert, notamment par le biais de son système nerveux : les stimuli émis par l'environnement sont indispensables à son fonctionnement », J.-C. Galloux, « Ébauche d'une définition juridique de l'information », *D.* 1994, p. 229, n° 25. V. aussi P. Kayser, *La protection de la vie privée par le droit,* 3e éd., Economica, 1990, n° 112, p. 212, selon qui « les personnes et les sociétés ont toujours eu besoin d'informations, mais ce besoin s'est accru dans les sociétés industrielles ».

[270] H. Croze, obs. ss Cass. crim., 29 avr. 1986, *JCP G* 1987, chron. 20788, n° 15. Pour justifier la situation d'exclusivité entre la personne et l'information, les auteurs invoquent souvent la jurisprudence concernant le vol d'information, v. not. Cass. crim., 12 janv. 1989, n° 87-82.265, *Bull. crim.* 1989, n° 14, p. 38 ; Cass. crim., 22 oct. 2014, n° 13-82.630, *NBP*. Sur le vol d'information, v. L. de Leyssac, « Une information seule est-elle susceptible de vol ou d'une autre atteinte juridique aux biens ? », *D.* 1985, p. 43 s. Pour autant, et comme le remarquent Mesdames Valérie-Laure Benabou et Judith Rochfeld, « des arrêts tranchent aussi en sens contraire (…). Récemment, en 2013, le tribunal de grande instance de Créteil a écarté la qualification de vol de données en cas de "téléchargement et [d']enregistrement sur plusieurs supports de fichiers informatiques », V.-L. Benabou et J. Rochfeld, *À qui profite le clic ? Le partage de la valeur à l'ère numérique*, Odile Jacob, 2015, p. 55.

[271] Pour une critique très complète des thèses patrimoniales de l'information, v. A. Lucas, J. Devèze et J. Frayssinet, *Droit de l'informatique et de l'Internet*, PUF, 2001, nos 470 s., spéc. p. 271.

[272] J. Passa, « La propriété de l'information, un malentendu ? », *Dr. et Pat.* 2001, n° 91, p. 65. V. dans le même sens, sur la propriété des données et le droit de la propriété intellectuelle, P. Bernt Hugentholtz, « Propriété des données », in *Mélanges M. Vivant,* Dalloz, 2020, p. 205 s., spéc. p. 207.

inventeurs ou des auteurs) et l'intérêt général qui bénéficie de la libre circulation de ces œuvres ou inventions : c'est une des raisons qui expliquent qu'ils ont un caractère *temporaire*[273]. La reconnaissance d'un droit de propriété sur l'information, dont le caractère est par nature perpétuel[274], remettrait en cause l'équilibre recherché et priverait donc ces droits spéciaux de toute utilité. Malgré les limites certaines affectant les théories patrimoniales de l'information, celles-ci ont prospéré et se sont développées à l'égard des données.

73. La substitution de la notion de donnée à celle d'information. Depuis le début des années 2000, la notion de donnée a progressivement remplacé, dans le discours juridique, celle d'information. Cela est particulièrement flagrant dans tous les domaines en lien avec l'informatique. Ce glissement s'explique notamment par la neutralité de ce terme et par sa dimension mathématique implicite[275]. En dépit de légères différences, les notions d'information et de donnée restent très proches et sont souvent utilisées comme des synonymes[276]. Cette proximité a incité quelques auteurs à étendre les thèses patrimoniales de l'information au bénéfice des données, particulièrement pour les données à caractère personnel.

74. Les données personnelles qualifiées comme des biens. Une partie de la doctrine, notamment inspirée par les propositions de Pierre Catala, envisage depuis quelques années de patrimonialiser les données à caractère personnel en leur reconnaissant la qualification de « biens »[277]. Selon ces auteurs, aucun obstacle juridique ne s'opposerait à la consécration d'un droit réel sur les données personnelles[278]. Au contraire même, une telle reconnaissance devrait être encouragée

---

[273] A. Lucas, J. Devèze et J. Frayssinet, *Droit de l'informatique et de l'Internet*, PUF, 2001, n° 472, spéc. p. 273.
[274] F. Terré et P. Simler, *Droit civil. Les biens*, 10e éd., Dalloz, 2018, n° 150, p. 154.
[275] V. *supra*, n° 59.
[276] V. *supra*, n° 58.
[277] V. not F. Zenati-Castaing et T. Revet, *Manuel de droit des personnes*, PUF, 2006, n° 377, p. 332 : « la maîtrise que le droit au respect de la vie privée confère sur les données relatives à l'existence personnelle est un rapport de propriété » ; T. Revet, « La propriété de la personnalité », *Gaz. Pal.* 2007, n° 139, p. 49 ; A. Bensoussan, « La propriété des données », *Blog Le Figaro,* 18 mai 2010. Cette vision a été réaffirmée en 2010 dans les cahiers IP, innovation et prospective, de la CNIL, « Vie privée à l'horizon 2020. Paroles d'experts », n° 1, 2010, p. 47 s., A. Bensoussan, « À terme, le droit de valoriser ses propres données apparaît inéluctable », *RLDI* 2018, n° 153, p. 54 ; J. Attali, « Être propriétaire de soi », *L'Express*, 18 févr. 2013 ; L. Parisot, A. Jardin *et al.*, « Nos "données personnelles" nous appartiennent : monétisons-les ! », *Le Monde* 5 févr. 2018 ; M. Anahory, « Il faut inventer un droit patrimonial sur ses données de santé », *Le Monde* 11 janv. 2019 ; M. Destreguil, « Plaidoyer en faveur d'une approche propriétariste des données personnelles », *Revue juridique personnes et famille* 2019, n° 3, p. 5, § 31. Comp. not. F. Mattatia et M. Yaïche, « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? », *RLDI* 2015, n° 115, p. 63.
[278] M. Destreguil, « Plaidoyer en faveur d'une approche propriétariste des données personnelles », *Revue juridique personnes et famille* 2019, n° 3, p. 5, § 31.

du fait de ses opportunités et avantages. Tout d'abord, elle apporterait aux individus un meilleur contrôle à l'égard de leurs données[279]. En effet, le droit de propriété serait l'outil indiqué pour assurer un tel contrôle, dès lors qu'il octroie à son titulaire la maîtrise totale de la chose : le pouvoir de l'utiliser (*usus*) ; le pouvoir d'en jouir (*fructus*) ; et enfin, le pouvoir d'en disposer (*abusus*)[280]. Utilement mobilisés, ces pouvoirs favoriseraient, selon ces auteurs, l'exploitation des données et organiseraient le partage de leur valeur[281]. Ensuite, la création d'un marché des données participerait à rééquilibrer les rapports de pouvoir entre les plateformes et leurs utilisateurs[282]. Dotés d'un capital, les individus pourraient s'allier et mieux faire valoir leurs droits[283]. Enfin, cette reconnaissance s'inscrirait dans un mouvement déjà entamé par le règlement européen par lequel les personnes se sont vues reconnaître un droit à la portabilité sur leurs données[284]. Pour autant, bien que séduisante à première vue, cette thèse fait l'objet de critiques.

75. Critiques des théories patrimoniales de la donnée à caractère personnel. Plusieurs auteurs ont critiqué l'application des théories patrimoniales aux données à caractère personnel[285]. La reconnaissance d'un droit de propriété sur les données,

---

[279] M. Destreguil, « Plaidoyer en faveur d'une approche propriétariste des données personnelles », *Revue juridique personnes et famille* 2019, nº 3, p. 5, § 33 ; L. Léger (dir.), *Mes data sont à moi. Pour une patrimonialité des données personnelles*, Génération Libre, janv. 2018.

[280] J. Rochfeld, *Les grandes notions du droit privé,* 2e éd., PUF, 2013, *Vº* « La propriété », nº 5, p. 275. Déjà au sujet du droit sur le nom, une partie de la doctrine a proposé de le qualifier comme un droit de propriété, v. sur l'exposé de cette doctrine, F. Terré et D. Fenouillet, *Droit civil. Les personnes*, 8e éd., Dalloz, 2012, nº 184, p. 184.

[281] Sur la réification des éléments de la personnalité, v. par ex., B. Edelman, « De la propriété-personne à la valeur-désir », *D.* 2004, p. 155. Comp. not. M. Bernelin, « La patrimonialisation des données personnelles : entre représentation(s) et réalité(s) juridiques, *JCP G* 2019, nº 46, doctr. 1172, § 14 ; Y. Poullet, « Le fondement du droit à la protection des données nominatives : "propriété ou liberté" », *Nouvelles technologies et propriété*, actes du colloque tenu à Montréal, 9 et 10 nov. 1989, E. Mackaay (dir.), Litec, 1991, p. 175 s., nº 6, spéc. p. 184.

[282] Comme le remarquait déjà Monsieur Michel Vivant en 1993, la CNIL n'hésite pas à reconnaître la « valeur marchande de l'information nominative », v. M. Vivant, « Le patronyme saisi par le patrimoine », in *Mélanges A. Colomer*, Litec, 1993, p. 517 s., nº 15.1, spéc. p. 529. La CNIL semble avoir confirmé cette interprétation en clôturant sans sanction ni mise en demeure la procédure qu'elle avait lancée dans le courant de l'année 2020 contre l'entreprise Tadata qui monétise les données à caractère personnel des personnes entre 15 et 25 ans, v. O. Chicheportiche, « Feu vert de la CNIL pour Tadata, l'application qui monétise les données des jeunes », *BFMTV* 6 oct. 2020.

[283] L. Léger (dir.), *Mes data sont à moi. Pour une patrimonialité des données personnelles*, Génération Libre, janv. 2018, p. 10.

[284] M. Bernelin, « La patrimonialisation des données personnelles : entre représentation(s) et réalité(s) juridiques, *JCP G* 2019, nº 46, doctr. 1172, § 3, L. Léger (dir.), *Mes data sont à moi. Pour une patrimonialité des données personnelles*, Génération Libre, janv. 2018, p. 78 s.

[285] Pour Monsieur Yves Poullet, la thèse du droit de propriété ou des droits réels comme fondement justificatif des législations sur la protection des données « apparaît à la fois erronée, dangereuse et incapable d'expliquer l'évolution du débat de la protection des données, v. Y. Poullet, « Le fondement du droit à la protection des données nominative : "propriété ou libertés" », *Nouvelles technologies et propriété*, actes du colloque tenu à Montréal, 9 et 10 nov. 1989, E. Mackaay (dir.), Litec, 1991, p. 175 s., nº 13, spéc. p. 184 ; plus récemment, v. Y. Poullet, « La "propriété" des données. Balade au "pays des merveilles" à l'heure du *big data* », in *Mélanges M. Vivant*, 2020, Dalloz, p. 339 s. Pour des critiques de ces thèses, v. not. J. Rochfeld, « Contre l'hypothèse de la qualification des données personnelles comme des biens », in *Les biens numériques,* dir. E. Netter et

particulièrement sur les données à caractère personnel, engendre plusieurs difficultés qu'il convient d'analyser succinctement[286]. D'abord, cette qualification entraîne un appauvrissement de la protection des personnes pouvant ressortir du droit des données à caractère personnel. En effet, en se limitant à la valeur patrimoniale des données, ces théories occultent un aspect, pourtant essentiel, de ces données : elles sont des composantes de l'identité ou de la personnalité de leur titulaire[287]. Leur traitement entraîne donc des risques de manipulation auquel le droit de propriété répond très mal[288]. À ce problème structurel s'ajoute également une série de difficultés pratiques. Par exemple, comment est désigné le bénéficiaire du droit de propriété : s'agit-il d'un droit à l'égard de la personne « productrice » des données, des opérateurs qui les traitent ou d'un système mixte[289] ? Lorsqu'il s'agit de données relatives à plusieurs personnes, comment ce système doit-il être organisé ? Par exemple, lorsque l'information concerne la vie sentimentale de deux individus ou qu'elle intéresse une famille entière, qui bénéficie du droit de propriété sur l'information [290]? Dans la continuité de cette interrogation se pose également la question de l'organisation de la défense de ce droit : qui doit être compétent pour déterminer la valeur des données ? Les « propriétaires » doivent-ils eux-mêmes négocier cette valeur ou doit-elle être déterminée par un tiers, telle qu'une autorité institutionnelle ou des groupements de consommateurs[291] ? L'exposé sommaire de ces questions illustre quelques-unes des

---

A. Chaigneau, CEPRISCA, 2015, p. 221 s. ; N. Ochoa, « Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition », *RFDA* 2015, p. 1157 ; v. aussi F. Mattatia et M. Yaïche, « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? », *RLDI* 2015, nº 115, p. 63 et nº 116, p. 41 ; P. Mouron, « Pour ou contre la patrimonialité des données personnelles », *La revue européenne des médias et du numérique* 2018, nº 46-47 ; M. Lanna, *La protection des données à caractère personnel à l'épreuve de l'automesure connectée*, th. Paris II, 2019, nºs 234 s., p. 184 s. V. déjà, P. Ancel, « La protection des données personnelles : aspects de droit privé français », *RID comp.* 1987, vol. 39, nº 3, p. 609, spéc. p. 621.

[286] Pour un aperçu de certaines de ces critiques, v. S. Gutwirth et G. Gonzalez Fuster, « L'éternel retour de la propriété des données : de l'insistance d'un mot d'ordre », in *Liber amicorum Yves Poullet*. *Law, norms and freedoms in cyberspace*, dir. E. Degrave, C. de Terwangne, S. Dusollier et R. Queck, Larcier, 2018, p. 117 s.

[287] J. Rochfeld, « Contre l'hypothèse de la qualification des données personnelles comme des biens », in *Les biens numériques,* dir. E. Netter et A. Chaigneau, CEPRISCA, 2015, p. 221 s., nº 10, spéc. p. 230 s. ; Y. Poullet, « Le fondement du droit à la protection des données nominative : "propriété ou libertés" », *Nouvelles technologies et propriété*, actes du colloque tenu à Montréal, 9 et 10 nov. 1989, E. Mackaay (dir.), Litec, 1991, p. 175 s., nº 5, spéc. p. 180 ; plus récemment, plus récemment, v. Y. Poullet, « La "propriété" des données. Balade au "pays des merveilles" à l'heure du *big data* », in *Mélanges M. Vivant*, 2020, Dalloz, p. 339 s.

[288] Sur les risques liés à la manipulation, v. *infra*, nºs 389 s.

[289] J. Rochfeld, « Contre l'hypothèse de la qualification des données personnelles comme des biens », in *Les biens numériques,* dir. E. Netter et A. Chaigneau, CEPRISCA, 2015, p. 221 s., nº 6, spéc. p. 227. Sur les difficultés liées à la propriété commune, v. F. Masson, *La propriété commune*, th. Paris I, 2016. En matière de correspondances, leur propriété serait liée à son transfert, v. V. Peltier, *Le secret des correspondances,* th. Aix-Marseille, 1998, PUAM, nº 110, p. 131 s. À l'heure de l'instantanéité de la transmission, une telle approche peut être remise en cause.

[290] Par exemple, si l'une des personnes consent et que l'autre ne consent pas, le droit de propriété répond relativement mal aux partages de la propriété de la donnée.

[291] L'entreprise Tadata, qui propose aux jeunes de patrimonialiser leurs données personnelles, détermine seule et de manière opaque le prix des données de ses utilisateurs, v. Tadata, « Foire aux questions ».

difficultés liées aux thèses patrimoniales. Un autre courant doctrinal, auquel nous souscrivons, analyse plutôt la qualification de la donnée sous l'angle personnaliste.

B. Les doctrines personnalistes

76. Le personnalisme. Pour Emmanuel Mounier, l'un des théoriciens du personnalisme, « la personne n'est pas un objet. Elle est même ce qui dans chaque homme ne peut être traité comme un objet »[292]. Ainsi, parler de doctrines juridiques personnalistes revient à placer l'intérêt de la personne (au sens d'être individuel et d'être social[293]) au centre des développements. En pratique, il semble y avoir autant de doctrines personnalistes que d'auteurs pour les défendre[294]. Toutefois, l'angle sous lequel sont appréhendés les enjeux étudiés est celui de l'intérêt de la *personne*.

77. Le principe de libre circulation de l'information. Par principe, l'intérêt de la collectivité impose la non-monopolisation de l'information, et celle-ci doit donc circuler librement[295]. Cette libre circulation de l'information est consubstantielle à l'existence des libertés individuelles et collectives, mais aussi à la création, à la science, et au développement humain[296]. La Déclaration universelle des droits de l'homme consacre ainsi, dans son article 19, que « tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui *de chercher, de recevoir et de répandre*, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit »[297].

---

[292] E. Mounier, *Le personnalisme,* PUF, 2010, p. 4. Le personnalisme est une philosophie éthique dont la valeur principale est le respect de la personne qui se situe comme une voie humaniste entre le capitalisme libéral et le marxisme.

[293] « Il y a en tout homme vivant en société l'être individuel et l'être social, pris en considération par le groupe et, à ce titre, traité comme sujet de droit », F. Terré et D. Fenouillet, *Droit civil. Les personnes*, 8e éd., Dalloz, 2012, no 9, p. 9.

[294] Pour un bref exposé des théories personnalistes en lien avec le droit à l'image, v. C. Deschanel, *Le droit patrimonial à l'image : émergence d'un nouveau droit voisin du droit d'auteur*, th. Aix-Marseille, 2017, nos 66 s., p. 51 s.

[295] N. Mallet-Poujol, « Appropriation de l'information : l'éternelle chimère », *D.* 1997, p. 330, nos 6 s. D'ailleurs, en matière incorporelle, la propriété constituerait l'exception et l'usage commun la règle, v. F. Zenati et T. Revet, *Les biens*, 3e éd., PUF, 2008, no 2, p. 20 ; J.-M. Mousseron, « Valeurs, biens, droits », in *Mélanges A. Breton et F. Derrida*, Dalloz, 1991, p. 277 s., no 11, spéc. p. 281. ; M. Vivant et A. Lucas, « Droit de l'informatique (suite) », *JCP E*, 1990, p. 15761, no 18.

[296] Selon certains auteurs, la liberté individuelle serait le compas véritable de la qualification des données, v. Y. Poullet, « Le fondement du droit à la protection des données nominative : "propriété ou libertés" », *Nouvelles technologies et propriété*, actes du colloque tenu à Montréal, 9 et 10 nov. 1989, E. Mackaay (dir.), Litec, 1991, p. 175 s., no 13, spéc. p. 184.

[297] De même, l'article 10 paragraphe premier de la Convention européenne de sauvegarde des droits de l'homme dispose que le droit à la liberté d'expression « comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière ». Pour Monsieur Nicolas Ochoa, « sans cette liberté de principe, la liberté d'expression n'aurait plus de portée pour peu qu'elle véhicule des informations relatives à des personnes nommément désignées, de même que la liberté de communication par téléphone ou par Internet, dans la mesure où il est par

78. Les données et le droit de propriété intellectuelle. En vertu du principe selon lequel les idées sont de libre parcours, le droit de la propriété intellectuelle exclut les idées et les informations brutes de son champ d'application[298]. Seule la forme originale ou innovante sous laquelle elles se sont exprimées leur permet de prétendre à une éventuelle protection[299]. Ces principes se justifient aisément : il s'agit de préserver la création, la connaissance et la liberté d'expression.

79. L'application du principe de libre circulation des informations aux données. Rien ne s'oppose à l'extension du principe de libre circulation de l'information au bénéfice des données. Au contraire, cette extension est cohérente dès lors que la donnée est la source de l'information puisqu'elle la précède[300]. Ainsi, puisque la donnée est l'élément brut qui compose l'information, le principe de libre circulation lui est également applicable. D'ailleurs, plusieurs fondements juridiques mettent en œuvre ce principe, notamment la liberté d'accès aux documents administratifs[301] ou encore la libre circulation des données à caractère non personnel récemment sanctifiée dans le règlement européen 2018/1807[302].

80. L'encadrement des restrictions à la libre circulation des données. En plaçant l'intérêt des personnes au centre des analyses relatives aux données, il apparaît essentiel de leur garantir un principe de libre circulation. En effet, une société libre est une société dans laquelle la donnée peut circuler librement et être utilisée par tous. Pour autant, il arrive que l'intérêt de la société soit supplanté par un intérêt individuel. Dans ce cas, l'accès à ces données doit alors être restreint. C'est le cas notamment des

---

nature délicat de faire un tri préalable entre la communication d'informations personnelles ou non. La liberté de prestation de services s'en trouverait pareillement handicapée dans la mesure où de telles prestations impliquent de plus en plus par principe un traitement, même minimal, des données personnelles des clients », v. N. Ochoa, « Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition », *RFDA* 2015, p. 1157.

[298] En droit de la propriété intellectuelle, c'est un principe fondamental que les idées (et donc les données) sont en elles-mêmes de libre parcours, v. H. Desbois, *Le droit d'auteur en France,* Dalloz, 3e éd., 1978, p. 22 ; v. aussi C. Caron, « L'adage "les idées sont de libre parcours" utilisé pour sanctionner le plaideur paresseux », *CCE* 2013, no 4, comm. 40. Le droit de propriété littéraire et artistique distingue bien entre l'information « brute de collecte » et l'œuvre, v. not. M. Vivant et J.-M. Bruguière, *Droit d'auteur et droits voisins*, 4e éd., Dalloz, 2019, nos 150 s., p. 197 s.

[299] Une donnée traitée sous un angle original peut être protégée au titre du droit d'auteur ; une invention fondée sur une donnée peut être protégée sur le fondement du droit des brevets, v. P.-Y. Gautier, *Propriété littéraire et artistique*, 11e éd., PUF, 2019, nos 37 s., p. 52 s.

[300] V. *supra*, no 59.

[301] Livre III du code des relations entre le public et l'administration.

[302] Règlement UE no 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, *JOUE* 28 nov. 2018, L-303/59, p. 59 s.

données ayant un lien particulier avec la personne, telles que les données à caractère personnel ou celles traitées sous un angle original. Ainsi, l'éventuelle protection juridique de ces données provient, non pas de la donnée *per se,* mais plutôt du lien particulier qu'elle entretient avec la personne[303].

81. Les données en rapport avec les personnes physiques. Pour Madame Judith Rochfeld, il ne fait pas de doute que les données personnelles sont des éléments de la personnalité : « elles émanent des individus, révèlent leur identité et participent de leurs comportements »[304]. En tant que tels, « seule une vision personnaliste des données (…) semble donc à même de traduire la texture de la donnée personnelle et de porter ces impératifs de protection » des personnes contre une circulation sans limite de leurs données[305]. Ainsi, la qualification de données personnelles tendrait plutôt vers une logique de droits inaliénables, plutôt que vers une logique patrimoniale[306].

La plupart des auteurs des théories personnalistes ne nient pas qu'un attribut de la personnalité puisse avoir une valeur, mais ils considèrent que cette valeur est mise en œuvre par un mécanisme différent de celui du droit réel[307]. À l'instar du principe de non-patrimonialité du corps humain, de ses éléments et de ses produits[308], les droits qu'une personne a sur ses données sont des droits extrapatrimoniaux, mais sont quand

---

[303] J.-C. Galloux, « Ébauche d'une définition juridique de l'information », *D.* 1994, p. 229, nº 10.

[304] Madame Judith Rochfeld considère que ce rattachement de la donnée à la personne doit être fait par la reconnaissance d'un droit fondamental à l'autodétermination informationnelle, v. J. Rochfeld, « Contre l'hypothèse de la qualification des données personnelles comme des biens », in *Les biens numériques,* dir. E. Netter et A. Chaigneau, CEPRISCA, 2015, p. 221 s., nº 11, spéc. p. 231. Dans le même sens, v. Y. Poullet, « Le fondement du droit à la protection des données nominative : "propriété ou libertés" », *Nouvelles technologies et propriété*, actes du colloque tenu à Montréal, 9 et 10 nov. 1989, E. Mackaay (dir.), Litec, 1991, p. 175 s., nº 5, spéc. p. 180 ; plus récemment, v. Y. Poullet, « La "propriété" des données. Balade au "pays des merveilles" à l'heure du *big data* », in *Mélanges M. Vivant*, 2020, Dalloz, p. 339 s., nº 6, spéc. p. 343. Cette conception est également celle retenue par le Conseil d'État dans son rapport de 2014, Conseil d'État, « Le numérique et les droits fondamentaux », *Rapport Public 2014*, La Documentation française, 2014, p. 267 s. V. déjà l'idée selon laquelle le droit au nom est une forme de la protection de l'intimité de chacun, E. Agostini, « La protection du nom patronymique et la nature du droit au nom », *D.* 1973, p. 313.

[305] J. Rochfeld, « Contre l'hypothèse de la qualification des données personnelles comme des biens », in *Les biens numériques,* dir. E. Netter et A. Chaigneau, CEPRISCA, 2015, p. 221 s., nº 10, spéc. p. 231.

[306] F. Mattatia et M. Yaïche, « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? », *RLDI* 2015, nº 116, p. 41, spéc. p. 44. Pour Madame Cécile Pérès, l'« approche patrimoniale cadre mal avec la dimension personnaliste du système juridique français et européen de protection des données personnelles. En effet, la protection des données personnelles se rattache à celle du droit au respect à la vie privée vu comme un droit de la personnalité et, sur le plan européen, au droit fondamental garanti par l'article 8 de la Convention européenne des droits de l'homme et par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne », C. Pérès, « Les données à caractère personnel et la mort. Observations relatives au projet de loi pour une République numérique », *D.* 2016, p. 90, nº 12.

[307] L. Marino, « La patrimonialisation du nom, de la voix et de l'image », in *Traité de droit de la presse et des médias*, dir. B. Beignier, B. de Lamy et E. Dreyer, LexisNexis, 2009, nº 1716, p. 997. À ce propos, Monsieur Grégoire Loiseau remarquait que ce n'est pas parce qu'un objet est indisponible qu'il ne peut pas faire l'objet d'une convention, G. Loiseau, *Le nom, objet d'un contrat*, th. Paris I, 1995, LGDJ, nºs 7 s., p. 7 s.

[308] La règle de non-patrimonialité du corps humain est posée par l'article 16-1 alinéa 3 du code civil, v. *Rép. civ.* Dalloz, *Vº* « Corps humain », par J. Penneau et E. Terrier, 2019, nº 55.

même des droits[309]. Les théories personnalistes préservent donc l'essence extrapatrimoniale des droits sur les données à caractère personnel, tout en admettant la validité des contrats les concernant[310].

82. Une approche personnaliste. En qualifiant la donnée en fonction des champs et liens qu'elle entretient avec la personne, c'est une approche centrée sur la personne qui est retenue. Selon cette conception, la donnée est vue comme un vecteur de libertés et non pas comme une valeur patrimoniale.

L'opposition entre ces théories témoigne du caractère vaste de la notion de donnée à caractère personnel.

C. Une controverse illustrant l'étendue de la notion de donnée

83. Une vision politique de la personne. L'opposition entre la vision patrimoniale et la vision personnaliste des données reflète en réalité deux conceptions politiques de la personne : la personne comme source de valorisation[311] et la personne comme sujet de droit[312]. Prudents, les législateurs français et européen n'ont pas tranché entre ces deux visions[313]. Au contraire, l'analyse des textes applicables montre qu'ils

---

[309] F. Terré et D. Fenouillet, *Droit civil. Les personnes*, 8e éd., Dalloz, 2012, nº 61, p. 67. V. déjà sur les droits de la personnalité, E.-H. Perreau, « Les droits de la personnalité », *RTD civ.* 1909, p. 501 ; P. Malaurie, « Les droits de la personnalité en 2003 », in *Mélanges A. Decocq,* Litec, 2004, p. 469 s., nº 1, spéc. p. 469 ; F. Terré et P. Simler, *Droit civil. Les biens*, 10e éd., Dalloz, 2018, nº 28, p. 36. Comp. P. Ancel, *L'indisponibilité des droits de la personnalité. Une étude critique des droits de la personnalité,* th. Dijon, 1978 ; G. Loiseau, « Les droits patrimoniaux de la personnalité en droit français », *Revue de droit de McGill* 1997, vol. 42, p. 319 s. Sur les contrats relatifs à des droits de la personnalité, v. *infra*, nº 351.

[310] La non-appropriation de l'information personnelle n'exclut pas la possibilité d'une exploitation commune ou individuelle et un contrôle de l'usage effectué par les tiers sur cette information, v. M. Cornu, F. Orsi et J. Rochfeld (dir.), *Dictionnaire des biens communs*, PUF, 2017, *Vº* « Information (approche juridique) ». Pour une critique de ces théories, v. C. Deschanel, *Le droit patrimonial à l'image : émergence d'un nouveau droit voisin du droit d'auteur*, th. Aix-Marseille, 2017, nos 70 s., p. 54 s.

[311] Pour Monsieur Thierry Revet, « le corps est et n'est qu'une chose », laquelle ainsi que « ses composants et ses produits, sont dans le commerce juridique : ils sont appropriés ». Cette commercialité trouve une limite (relative) dans la nullité des conventions ayant pour effet de conférer une valeur patrimoniale au corps, v. T. Revet, « Le corps humain est-il une chose appropriée ? », *RTD civ.* 2017, p. 587. D'ailleurs, la conception de la propriété de l'homme se retrouve dans les analyses libertariennes, v. R. Nozick, *Anarchie, État et utopie,* PUF, 1974. Robert Nozick s'inspire de la conception de la liberté individuelle comme propriété, telle qu'elle est développée par le philosophe anglais John Locke au XVIIe siècle.

[312] V.-L. Benabou et J. Rochfeld, *À qui profite le clic ? Le partage de la valeur à l'ère numérique*, Odile Jacob, 2015, p. 63.

[313] Le gouvernement français a toutefois affirmé que la consécration par l'article 16 du projet de loi pour une République numérique d'un droit à la libre disposition de ses données, « permet de clarifier l'absence de propriété sur les données » et de souligner qu'il est « préférable de créer un droit rattaché à la personne, c'est-à-dire un droit de la personnalité », v. Gouvernement, « Explication des articles », *republique-numerique.fr*. Parfois, le législateur européen énonce clairement que les données à caractère personnel « ne peuvent être considérées comme des marchandises », v. cons. 24 de la directive UE nº 2019/770 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques, *JOUE* 22 mai 2019, L-136/1, p. 1 s. À l'inverse, le législateur européen invoque parfois certaines théories du droit patrimonial dans le domaine de la protection des données personnelles, en considérant que la notion de rémunération doit comprendre les cas dans lesquels un opérateur demande à l'utilisateur de fournir des données personnelles, considérant 16 de la directive UE nº 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (refonte), *JOUE* 17 déc. 2018,

entretiennent cette confusion : ils reconnaissent des régimes de circulation des données, tout en organisant une protection de la personne[314].

Devant la variété de ce que recouvre la notion de donnée, le juriste doit admettre son ampleur et son étendue. Les thèses patrimoniales encouragent une vision réifiée de la personne et de ses éléments. À l'opposé, les thèses personnalistes reconnaissent la valeur fondamentale de la donnée pour la société et son besoin de circulation. Selon ces thèses, seules certaines données doivent être exclues de ce principe de libre circulation, notamment dans le but de protéger des intérêts individuels. Une telle conception nous paraît plus en phase avec le besoin de protection des personnes.

84. Les difficultés pour s'entendre sur une qualification unique de la donnée. L'étude des différents courants relatifs à la qualification de donnée montre le caractère protéiforme de cette notion[315]. Elle est si large qu'elle peut faire l'objet de qualifications juridiques très différentes : patrimoniale et personnalisme, valorisation et protection.

En définitive, la notion de donnée apparaît presque sans limite : plus large que celle d'information, souvent inhérente aux documents et aux fichiers, elle s'applique amplement. Elle embrasse des qualifications juridiques diverses qui trouvent leurs fondements dans une réalité tout aussi éclectique ; pour le dire trivialement, la donnée est partout et sa notion juridique reflète cette universalité.

En plus d'être une donnée, la donnée à caractère personnel doit aussi se rapporter à une personne physique.

L-321/36, p. 36 s. La Commission européenne semble aussi avoir récemment pris position en faveur d'une approche mercantile des données à caractère personnel, v. Commission européenne, COM (2020) 66, « Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions. Une stratégie européenne pour les données », 19 févr. 2020. Pour une analyse de l'errance du législateur européen entre ces qualifications, v. N. Martial-Braz, « Les nouveaux droits des individus consacrés par la loi pour une République numérique. Quelle articulation avec le Règlement européen ? », *Dalloz IP/IT* 2016, p. 525.

[314] J. Rochfeld, « Contre l'hypothèse de la qualification des données personnelles comme des biens », in *Les biens numériques,* dir. E. Netter et A. Chaigneau, CEPRISCA, 2015, p. 221 s., nº 5, spéc. p. 225 s. Pour une étude récente sur la position européenne en la matière, v. S. Carre, « Libre circulation des données, propriété et droit à l'information : à propos du règlement (UE) 2018/1807 du 14 novembre 2018 », *Dalloz IP/IT* 2020, p. 228.

[315] La notion de donnée serait si large qu'il conviendrait, selon certains auteurs, d'élaborer un droit commun de la donnée, v. M. Bourgeois et L. Thibierge, « Droit de la donnée : plaidoyer pour un régime général », *JCP E* 2020, nº 20, p. 1207, § 6.

SECTION II – LE CARACTÈRE PERSONNEL : LE RAPPORT AVEC UNE PERSONNE PHYSIQUE

85. Plan. Pour être qualifiée de donnée à caractère personnel, la donnée n'est pas seulement un contenu brut[316], elle doit aussi *concerner* une *personne physique*. Ainsi, deux autres éléments composent la notion. Il convient dans un premier temps de cerner les contours de la personne, au sens du droit des données à caractère personnel (§ I). Ensuite, il faut étudier le critère du rattachement, c'est-à-dire le lien unissant la donnée à une personne. Ce rattachement peut présenter des degrés différents (§ II).

§ I. La personne au sens du droit des données à caractère personnel

86. L'absence de définition de la personne physique par le droit des données à caractère personnel. Pour être qualifiée de donnée à caractère personnel, la donnée doit se rapporter à une personne physique. En dépit du caractère central de la notion de personne physique, aucun des législateurs du droit des données à caractère personnel n'a pris le soin de la définir, au sens de ce droit. Plusieurs hypothèses peuvent être avancées pour expliquer un tel mutisme. Tout d'abord, il est envisageable de considérer que cette notion serait parfaitement alignée sur celle du droit civil, selon laquelle la personne physique est l'être humain auquel on a attribué la jouissance de droits[317]. Dès lors, nul besoin de définir la personne physique spécifiquement puisqu'il suffit de se référer au droit civil. Ensuite, il est possible de penser que le législateur a souhaité laisser une marge d'appréciation aux juges pour adapter la notion de personne physique aux évolutions sociétales et technologiques. La notion de personne physique pourrait ici être légèrement différente de celle classiquement retenue en droit civil. Enfin, il est envisageable d'imaginer que le législateur européen, confronté à l'absence de consensus sur cette notion entre les États membres, s'est abstenu de la définir pour laisser une plus grande souplesse aux législateurs nationaux et permettre une meilleure réception de la matière dans les droits internes[318]. À l'étude, il apparaît que la notion

---

[316] C. Shannon, « A mathematical theory of communication », *The Bell System Technical Journal* 1948, vol. 27, p. 379.
[317] J. Carbonnier, *Droit civil,* vol. 1, *Introduction. Les personnes. La famille, l'enfant, le couple*, PUF, 2004, n° 193, p. 373 : « Les personnes, au sens juridique du terme, sont les êtres capables de jouir de droits ; ce sont, d'une expression équivalente, les sujets de droit ». V. aussi F. Terré et D. Fenouillet, *La famille,* 8e éd., Dalloz, 2012, n° 9, p. 9, pour qui « d'emblée, on peut dire que les personnes, ce sont les sujets de droit ».
[318] Pour un recueil d'études liées à la notion de personne en droit européen, v. *Constructing the person in EU law : rights, roles, identities,* dir. L. Azoulai, S. Barbou des Places et E. Pataut, Bloomsbury Publishing, 2016.

de « personne physique », au sens du droit des données à caractère personnel, n'est pas parfaitement alignée sur celle retenue traditionnellement en droit civil[319].

87. Plan. Si la définition de donnée à caractère personnel vise *a priori* les personnes physiques (A), cela n'empêche pas toujours les personnes morales de s'y glisser (B).

A. Une notion large de personne physique

88. La personne physique en droit civil. Étymologiquement, le terme de personne découle du latin *persona*, qui désigne le masque de théâtre permettant à l'acteur de jouer le rôle désigné par ce masque[320]. C'est bien là la fonction de la personnalité juridique : permettre à un individu de jouer un rôle d'acteur[321]. Selon une doctrine majoritaire, la personne physique serait l'« être humain, tel qu'il est considéré par le Droit ; la personne humaine prise comme sujet de droit »[322]. Ainsi, la personne physique est avant tout un être de chair et de sang, apte à devenir titulaire de droits[323]. La notion de personne se structure donc autour de l'aptitude de celle-ci à participer à la vie juridique[324]. Cette notion est intrinsèquement liée à celle de personnalité juridique[325].

89. La personnalité juridique. Pour déterminer les contours de la personne physique, il est nécessaire de s'intéresser à la notion de personnalité juridique[326]. En

---

[319] Pour Madame Marie-Anne Frison-Roche, dès lors que l'on ne dispose pas d'une véritable définition légale, « il faut effectivement se rapporter à la pratique décisionnelle du Régulateur, droit par nature casuistique, qui a produit davantage de précisions, pour relever les points communs fournissant pour l'observateur les linéaments d'une définition », M.-A. Frison-Roche, « Penser le monde à partir de la notion de "donnée" », in *Internet, espace d'interrégulation*, dir. M.-A. Frison-Roche, Dalloz, 2016, p. 8.

[320] F. Gaffiot, *Dictionnaire Latin-Français*, Hachette, 2000, *V°* « Persōna », sens I, II et III.

[321] D'ailleurs, le terme de personne se décompose étymologiquement en *per* et *sonare* et signifie « ce par l'intermédiaire de quoi le son se manifeste », v. F. Terré et D. Fenouillet, *La famille,* 8e éd., Dalloz, 2012, n° 10, p. 10. Plus largement, sur la personnalité, v. A. Bertrand-Mirkovic, *La notion de personne (étude visant à clarifier le statut juridique de l'enfant à naître)*, th. Aix-Marseille, 2003, PUAM, nos 516 s., p. 264. Pour une analyse philosophique et politique de la notion de personne, v. C. Levy, *La personne humaine en droit*, th. Paris I, 2000, nos 24 s., p. 26 s.

[322] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *V°* « Personne », spéc. physique. Sur les controverses relatives à la définition de personne, v. N. Anciaux, *Essai sur l'être en droit privé*, th. Paris II, 2018, LexisNexis, nos 34 s.

[323] « Apte à être titulaire actif et passif de droits et à être protégé comme sujet de droit, tel est le statut de l'être doté de la personnalité juridique », F. Terré et D. Fenouillet, *La famille,* 8e éd., Dalloz, 2012, n° 15, p. 17. V. aussi, B. Teyssié, *Droit des personnes*, 21e éd., LexisNexis, 2019, n° 19, p. 19.

[324] C'est d'ailleurs ce qui distingue cette notion de celle de personne humaine, v. J. Rochfeld, *Les grandes notions du droit privé,* 2e éd., PUF, 2013, *V°* « La personne », n° 4, p. 17.

[325] J. Dabin, *Le droit subjectif*, Dalloz, 1952, réimpr. 2007, p. 111 s.

[326] Classiquement, la personnalité juridique « n'est pas seulement l'aptitude à recueillir des droits subjectifs (…) et à subir ceux d'autrui, mais, beaucoup plus largement, la vocation à être pris en compte dans les diverses situations définies et régies par le droit objectif », v. J.-L. Aubert et E. Savaux, *Introduction au droit et thèmes fondamentaux du droit civil*, 18e éd., Sirey, 2020, n° 197, p. 257.

principe, celle-ci s'acquiert par la naissance[327]. Avec elle, la personne jouit d'une personnalité lui permettant d'acquérir des droits mais aussi de supporter les obligations afférentes. Certains auteurs discutent de la possibilité de faire remonter avant la naissance le moment d'apparition de la personnalité juridique, mais une telle possibilité est rarement retenue[328]. Au cours de sa vie, une personne acquiert des droits et des aménagements sont fixés en fonction de son âge[329]. La personnalité juridique s'achève au moment de la mort, c'est-à-dire à l'arrêt de l'activité cérébrale[330]. Ainsi, en résumé, le droit civil considère, par principe, qu'une personne physique est un *être humain vivant*[331].

90. La personne physique en droit des données à caractère personnel. En droit des données personnelles, la notion de personne physique peut, dans certains cas, exister temporellement au-delà du début et de la fin de la personnalité juridique classiquement reconnue par le droit civil. En effet, certaines particularités sont à relever. Pour les personnes à naître d'abord (1), pour les personnes mortes ensuite (2), et pour ces deux catégories de personnes lorsque les informations concernent des personnes vivantes (3).

---

[327] Plus précisément, pour être considéré comme un sujet de droit, l'enfant doit être né vivant et viable, v. M. Fabre-Magnan et F. Brunet, *Introduction générale au droit,* PUF, 2017, nº 164, p. 223 s. ; J.-L. Aubert et E. Savaux, *Introduction au droit et thèmes fondamentaux du droit civil*, 18e éd., Sirey, 2020, nº 200, p. 260 ; J. Hauser, « Les bornes de la personnalité juridique en droit civil », *Dr. Fam.* 2012, nº 9, dossier 4.

[328] En se fondant sur les principes généraux du droit, la Cour de cassation reconnaît qu'il est possible de faire remonter l'acquisition de la personnalité juridique dès la conception de l'enfant toutes les fois où il y va de son intérêt. Il s'agit de la maxime *infans conceptus pro nato habetur quoties de commodis ejus agitur*, v. Cass. civ. 1re, 10 déc. 1985, nº 84-14.328, *Bull. civ.* 1985, I, nº 339, p. 305. Pour une présentation générale de ce principe, v. not. F. Terré et D. Fenouillet, *Droit civil. Les personnes*, 8e éd., Dalloz, 2012, nos 20 s., p. 23 s. Pour une étude des cas dans lesquels les effets de la personnalité juridique peuvent être rétroactifs, v. A. Bertrand-Mirkovic, *La notion de personne (étude visant à clarifier le statut juridique de l'enfant à naître)*, th. Aix-Marseille, 2003, PUAM, nos 612 s.

[329] C'est le cas, par exemple, pour la capacité à contracter, le droit de vote, la retraite ou encore le droit de candidater à certaines fonctions.

[330] *Rép. civ.* Dalloz, *Vº* « État et capacité des personnes – État », par I. Gallmeister, 2016 (actu. 2019), nº 56. Encore que la Cour de cassation ait précisé que le critère de la mort cérébrale n'a pas de portée générale, mais est limité à la finalité même de ce constat qui est de permettre un prélèvement d'organes, v. Cass. civ. 1re, 19 oct. 1999, nº 97-19.845, *Bull. civ.* 1999, I, nº 283, p. 184. V. déjà, l'arrêt *Milhaud* du Conseil d'État (CE Sec., 2 juill. 1993, *Milhaud*, nº 124960, *Lebon* p. 194), dont les principes ont été repris par un décret de 1996 (décret nº 96-1041 du 2 déc. 1996 relatif au constat de la mort préalable au prélèvement d'organes, de tissus et de cellules à des fins thérapeutiques ou scientifiques, *JORF* 4 déc. 1996, nº 282, p. 17615). Pour une étude détaillée de cette question, v. A. Bertrand-Mirkovic, *La notion de personne (étude visant à clarifier le statut juridique de l'enfant à naître)*, th. Aix-Marseille, 2003, PUAM, nos 341 s.

[331] Pour une étude sur le « chaos sémantique » qui habite le discours juridique lié à la personne physique, v. N. Anciaux, *Essai sur l'être en droit privé*, th. Paris II, 2018, LexisNexis, nº 40.

1. Les personnes à naître

91. Le principe d'exclusion des personnes à naître. Comme l'annonçaient Mesdames Catherine Labrusse-Riou et Florence Bellivier, « la condition juridique de l'être humain conçu et non encore né est, en droit contemporain, une des questions théoriques et pratiques les plus difficiles, les plus controversées et les plus agitées par l'actualité »[332]. Pourtant, en droit civil comme en droit des données à caractère personnel, certaines hypothèses requièrent une prise de position. Par principe, l'embryon ou le fœtus n'ont pas le statut de personne[333]. Ils n'ont donc pas la personnalité juridique et ne sont pas considérés comme des sujets de droit[334].

En droit des données à caractère personnel, une telle absence de statut questionne sur le sort des traitements effectués sur les données d'un embryon ou d'un fœtus. En effet, puisque ces données se distinguent de celles de la mère, il est possible de s'interroger sur les règles applicables à leurs traitements. Par principe, puisqu'elles ne se rapportent pas à une personne physique, ces données sont exclues de la notion de donnée à caractère personnel, et leurs traitements ne sont pas soumis à ce droit[335]. Pourtant, une telle exclusion est problématique, non seulement si cet embryon devient une personne physique, mais surtout pour l'intégrité de l'espèce humaine[336].

92. Les limites à l'exclusion de principe : l'intérêt de l'enfant. À l'instar de ce qui existe en droit de la famille, et plus spécifiquement en droit des successions, la maxime *infans conceptus* (…) devrait s'appliquer aux données liées aux embryons ou fœtus. En effet, réguler les traitements effectués sur les données des personnes à naître, et empêcher des traitements sauvages, est favorable à l'intérêt de l'enfant. En tout état de cause, fort heureusement, les recherches sur ces embryons demeurent encadrées par

---

[332] C. Labrusse-Riou et F. Bellivier, « Les droits de l'embryon et du fœtus en droit privé », *RID comp.* 2002, vol. 54, p. 579.
[333] Ils bénéficient néanmoins d'une protection spécifique propre à l'être humain, v. art. 16-4 du code civil. V. aussi, J. Rochfeld, *Les grandes notions du droit privé,* 2e éd., PUF, 2013, *Vo* « La personne », no 9, p. 28. Pour Madame Claire Neirinck, « l'embryon n'est ni une personne juridique, telle que la définit le code civil, ni une personne humaine, telle que la protège le code pénal », v. C. Neirinck, « L'embryon humain : une catégorie juridique à dimension variable ? », *D.* 2003, p. 841.
[334] F. Bellivier, *Droit des personnes*, LGDJ, 2015, no 222, p. 205. La Chambre criminelle de la Cour de cassation a conforté l'absence de personnalité juridique de l'embryon en affirmant que le fait de provoquer sa mort ne constitue pas un homicide, v. Cass. Ass. plén., 29 juin 2001, no 99-85.973, *Bull. crim.* 2001, no 165, p. 546 ; Cass. crim., 25 juin 2002, no 00-81.359, *Bull. crim.* 2002, no 144, p. 531. La Cour européenne des droits de l'homme a approuvé ce raisonnement qui ne viole pas le droit à la vie, CEDH 8 juill. 2004, *Vo* c. *France*, n° 53924/00, § 74 s.
[335] Pour un panorama de l'encadrement juridique de ces traitements, v. not. J.-C. Galloux et H. Gaumont-Prat, « Droits et libertés corporels », *D.* 2010, p. 604.
[336] L'article 16-4 du code civil interdit de « porter atteinte à l'intégrité de l'espèce humaine. Toute pratique eugénique tendant à l'organisation de la sélection des personnes est interdite ».

d'autres principes du droit, lesquels forment une sorte de bouclier protégeant par ricochet ces données si particulières. En effet, depuis 1994, des règles réglementent la recherche sur l'embryon et encadrent les traitements effectués sur ces données[337].

À ces difficultés relatives aux personnes à naître s'ajoutent également des difficultés liées aux personnes mortes.

2. Les personnes mortes

93. Le silence des textes. Planiol affirmait que « les morts ne sont plus des personnes ; ils ne sont plus rien »[338]. Après ce glaçant constat, il actait que « la personnalité se perd avec la vie »[339]. En toute logique, aucun texte ne reconnaît, au-delà de la mort, le bénéfice des droits de la personnalité[340]. Ainsi, l'article 9 du code civil ne dit rien sur un éventuel droit au respect de la vie privée des personnes décédées[341] ; quant à la loi Informatique et libertés ou la directive européenne 95/46, elles ne réservaient pas de place particulière aux données à caractère personnel des personnes décédées[342]. Suppléant le silence du législateur, les juges ont été chargés de déterminer les limites temporelles des actions relatives à ces droits.

94. L'absence de protection *post mortem* de la vie privée. Si la célèbre décision du tribunal de la Seine de 1858 relative au portrait de l'actrice Rachel avait pu laisser supposer une éventuelle reconnaissance d'une protection *post mortem* de la vie privée[343], il est désormais de jurisprudence constante que « le droit d'agir pour le

---

[337] V. loi n° 94-654 du 29 juill. 1994 relative au don et à l'utilisation des éléments et produits du corps humain, à l'assistance médicale à la procréation et au diagnostic prénatal, modifiée successivement par la loi n° 2004-800 du 6 août 2004, la loi n° 2011-814 du 7 juill. 2011, la loi n° 2013-715 du 6 août 2013 et la loi n° 2016-41 du 26 janv. 2016. Sur l'évolution de ce cadre juridique, v. not. A.-M. Leroyer, « Embryon. Recherche. Cellules souches », *RTD civ.* 2013, p. 895 ; L. Lambert-Garrel et F. Vialla, « L'exception devient principe : à propos de la recherche sur l'embryon et les cellules souches embryonnaires. Proposition de loi adoptée le 16 juillet 2013 », *D.* 2013, p. 1842. Pour une étude des liens entre la protection des informations nominatives et les lois bioéthiques, v. M.-C. Ponthoreau, « La protection des personnes contre les abus de l'informatique. À propos de la loi du 1er juillet 1994 relative au traitement des données nominatives ayant pour fin la recherche dans le domaine de la santé », *RFDA* 1996, p. 796.

[338] M. Planiol, *Traité élémentaire de droit civil*, t. 1, 11e éd., LGDJ, 1920, n° 371.

[339] M. Planiol, *Traité élémentaire de droit civil*, t. 1, 11e éd., LGDJ, 1920, n° 371.

[340] *JCl. comm.,* fasc. 34, « Droit au respect de la vie privée. Définition conceptuelle du droit subjectif », par J.-C. Saint-Pau, 2016 (actu. 2019), n° 40.

[341] Sur la question de la protection *post mortem* de la vie privée, v. D. Chauvet, *La vie privée. Étude de droit privé,* th. Paris-Sud, 2014, n° 487, p. 385.

[342] D'autres législateurs, notamment le législateur anglais, ont fait le choix d'exclure explicitement les personnes décédées du bénéfice de la protection des données personnelles, v. A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, n° 604, p. 256.

[343] Le ministère public avait déclaré dans ses conclusions, « quelque grande que soit une artiste, quelque historique que soit un grand homme, ils ont leur vie privée distincte de la vie publique, leur foyer domestique séparé de la scène et du forum. Ils peuvent vouloir mourir dans l'obscurité quand ils ont vécu, ou parce qu'ils ont vécu dans

respect de la vie privée ou de l'image s'éteint au décès de la personne concernée, seule titulaire de ce droit »[344]. Les auteurs s'accordent également pour affirmer que seuls les vivants ont une vie privée ; les morts, quant à eux, n'ont plus de personnalité, ni de vie, ce qui signifie que l'on ne saurait porter atteinte à leur vie privée, qui s'est éteinte à leur décès[345]. Ce principe ne concerne pas seulement le droit au respect de la vie privée mais l'ensemble des droits de la personnalité[346].

95. L'empreinte numérique des individus survivant à leur disparition physique. Avec l'utilisation intensive des services numériques, les situations dans lesquelles des données à caractère personnel survivent à une personne décédée sont de plus en plus courantes[347]. Quelques exemples illustrent la variété des données personnelles laissées par la personne : les photographies abandonnées sur un réseau social, les commentaires laissés sur un forum de discussion, les correspondances privées consignées dans une messagerie électronique. Se posent alors deux questions : d'abord celle de savoir si les données à caractère personnel d'une personne morte peuvent bénéficier d'une protection juridique ; et dans le cas où une telle protection était reconnue, qui devrait être chargé d'exercer les droits du *de cujus*.

96. L'action *post mortem* sur les données personnelles. Les textes européens et la loi française sont longtemps restés silencieux quant à l'effet du décès d'une personne sur le traitement de ses données. En l'absence de précisions législatives, ces données

---

le triomphe. Ils ont le droit de cacher à tous les yeux ces dernières scènes de la vie, ces dernières faiblesses ou ces dernières grandeurs, ces larmes de la famille, ces attendrissements suprêmes qui n'appartiennent qu'à eux. L'homme célèbre, messieurs, a le droit de mourir caché ; et si la famille, après le dernier soupir, veut faire reproduire ses traits pour elle seule, non, vous ne pouvez pas, au nom de la célébrité qui survit à la mort, toucher à ces choses », Trib. Seine, 16 juin 1858, *Rachel*, *D.* 1858, III, p. 62.

[344] V. parmi les nombreux arrêts Cass. civ. 1re, 14 déc. 1999, nº 97-15.756, *Bull. civ.* 1999, I, nº 345, p. 224 ; Cass. civ. 2e, 8 juill. 2004, nº 03-13.260, *Bull. civ.* 2004, II, nº 390, p. 329 ; Cass. civ. 1re, 15 févr. 2005, nº 03-18.302, *Bull. civ.* 2005, I, nº 86, p. 76 ; Cass. civ. 1re, 12 déc. 2006, nº 04-20.719, *Bull. civ.* 2006, I, nº 551, p. 491 ; Cass. civ. 1re, 4 févr. 2015, nº 14-11.458, *NPB*. Cette interprétation est également celle retenue par la CEDH, laquelle considère que « le principe voulant que les droits tirés de l'article 8 soient de nature non transférable et ne puissent donc être revendiqués par un parent proche ou un autre héritier de la victime immédiate », v. not. CEDH, 26 oct. 2000, *Sanles Sanles* c. *Espagne*, nº 48335/99 ; CEDH, 19 juill. 2012, *Koch* c. *Allemagne*, nº 497/09, § 79.

[345] E.-H. Perreau, « Des droits de la personnalité », *RTD civ.* 1909, p. 501, spéc. p. 526 ; P. Kayser, « Les droits de la personnalité. Aspects théoriques et pratiques », *RTD civ.* 1971, p. 445, nº 39 ; C. Caron, « Les morts n'ont pas de vie privée », *D.* 2000, p. 266. Classiquement, « le principe est que la protection de la vie privée cesse avec le décès, car les droits de la personnalité sont intransmissibles », v. P. Malaurie et L. Aynès, *Cours de droit Civil,* t. 2, *Les Personnes, les incapacités*, 5e éd., Cujas, 1999, nº 319. En revanche, il est admis que les héritiers peuvent agir lorsqu'ils éprouvent un préjudice personnel établi par l'atteinte à la vie privée du défunt, v. *Rép. civ.* Dalloz, *Vº* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), nos 156 s.

[346] B. Teyssié, *Droit des personnes*, 21e éd., LexisNexis, 2019, nº 264, p. 236. Il existe quelques exceptions à ce principe, M. Grimaldi, *Droit des successions,* 7e éd., LexisNexis, 2017, nos 74 s., p. 49 s.

[347] A. Favreau, « Mort numérique : précisions sur la nature et le régime du contrôle *post mortem* des données à caractère personnel collectées », *RLDI* 2016, nº 132, p. 36.

continuaient d'être traitées par les services numériques et les héritiers ne pouvaient pas y accéder[348].

Ce système a subi une première brèche en 2004, lors de la modification de la loi Informatique et libertés. Les héritiers se sont alors vu reconnaître le droit « d'exiger du responsable du traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence »[349]. Ainsi, le législateur a autorisé l'application, au-delà du décès d'une personne, de certains des principes de protection des données à caractère personnel[350]. Néanmoins, cette reconnaissance limitée ne répondait pas à l'ensemble des problèmes engendrés par le décès d'une personne. La CNIL[351] et la doctrine[352] ont donc dénoncé son champ d'application trop restreint et ont appelé de leurs vœux des modifications législatives.

97. La reconnaissance légale de droits *post mortem* sur les données à caractère personnel. En octobre 2016, le législateur français a répondu à cet appel en instaurant un nouveau système de gestion *post mortem* des droits sur les données à caractère personnel[353]. L'article 63 de la loi pour une République numérique a ainsi prévu le maintien provisoire des droits des personnes concernées dans deux situations :

(1) lorsque la personne a défini, au cours de sa vie, des directives concernant le traitement de ses données après son décès[354], et

(2) en l'absence de telles directives, il revient aux héritiers d'exercer ces droits pour organiser la succession et faire prendre en compte le décès par les responsables de traitement[355].

---

[348] Comme le remarquait Madame Cécile Pérès, « les professionnels du numérique se retranchent derrière leurs conditions générales censément acceptées par le défunt pour refuser à sa famille tout accès au contenu des comptes et toute transmission à ses héritiers de valeurs numériques », C. Pérès, « Les données à caractère personnel et la mort. Observations relatives au projet de loi pour une République numérique », *D.* 2016, p. 90, n° 5.
[349] Art. 40 de la loi n° 78-17 du 6 janv. 1978 telle que modifiée par la loi n° 2004-801 du 6 août 2004.
[350] Particulièrement le droit à la rectification et le droit à l'effacement des données.
[351] CNIL, « Mort numérique ou éternité virtuelle : que deviennent vos données après la mort ? », 29 oct. 2014. Pour une analyse de cette fiche pratique, v. A. Favreau, « Mort numérique : quel sort juridique pour nos informations personnelles ? », *RLDC* 2016, n° 132, p. 36.
[352] Les auteurs ont également discuté de l'opportunité de reconnaître un testament des dernières volontés numériques, v. A. Favreau, « Mort numérique : précisions sur la nature et le régime du contrôle *post mortem* des données à caractère personnel collectées », *RLDI* 2016, n° 132, p. 36 ; A. Mâzouz, « Être ou ne plus être, les volontés à l'origine de la mort numérique », in *Droit et réseaux sociaux*, dir. V. Ndior, Lextenso, 2015, p. 186 s. ; ou un mandat *post mortem* pour les données personnelles, v. C. Béguin-Faynel, « Héritage numérique & cadavre(s). Pour un testament des dernières volontés numériques », in *Traité des nouveaux droits de la mort*, t. 2, dir. M. Touzeil-Divina, M. Bouteille-Brigant et J.-F. Boudet, Lextenso, 2014, p. 67 s.
[353] Loi n° 2016-1321 du 7 oct. 2016 pour une République numérique. Pour une analyse de la mort numérique, et notamment du régime du maintien provisoire de l'exercice de certains droits sur les données personnelles, F. Bicheron, « La mort numérique », in *Mélanges M. Grimaldi*, Defrénois, 2020, p. 81 s., n°s 13, spéc. p. 87.
[354] Art. 85 § I de la loi n° 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance n° 2018-1125 du 12 déc. 2018.
[355] Art. 85 § II de la loi n° 78-17 du 6 janv. 1978 telle que modifié par l'ordonnance n° 2018-1125 du 12 déc. 2018.

Cette protection *post mortem* est toutefois limitée au seul exercice de certains des droits classiquement reconnus aux personnes concernées sur leurs données.

98. Une protection *post mortem* circonscrite aux droits des personnes sur leurs données. La protection instaurée par la loi pour une République numérique limite l'exercice des droits *post mortem* aux seuls droits des personnes concernées, notamment au droit d'accès, de rectification ou d'effacement[356]. Les autres principes de la matière, tels que le principe de conservation limitée ou celui de finalité, sont exclus de l'extension *post mortem* des droits. Ainsi, les responsables du traitement ont toujours la possibilité d'effectuer des traitements sans lien avec les finalités initiales[357] ou de partager les données personnelles des personnes décédées avec des tiers. Cette restriction est regrettable parce que les autres principes du droit des données à caractère personnel sont également importants pour l'effectivité de la protection des personnes résultant du droit des données à caractère personnel[358].

99. Une nuance à la conception classique de la fin de la personnalité. Selon une opinion doctrinale, la reconnaissance d'une telle protection *post mortem* apparaît « franchement inconciliable avec le principe selon lequel le droit au respect de la vie privée s'éteint au décès de la personne concernée, seule titulaire de ce droit »[359]. Cette transmission constitue une nouvelle brèche dans le principe d'intransmissibilité des droits de la personnalité et contribue au développement d'une conception renouvelée de la personne. Elle présente l'avantage de garantir une protection plus cohérente des personnes.

100. Rapprochements avec le droit au respect du corps humain ? La reconnaissance de droits *post mortem* sur les données s'inscrit dans un mouvement juridique s'éloignant de la césure tranchée, longtemps opérée par le droit, entre vie et

---

[356] Le second alinéa de l'article 84 de la loi n° 78-17 du 6 janv. 1978, telle que modifiée par l'ordonnance n° 2018-1125 du 12 décembre 2018, vise expressément les « droits mentionnés au chapitre II », c'est-à-dire les droits de la personne concernée.
[357] Par exemple, une compagnie d'assurance pourrait utiliser des données liées à la conduite de personnes ayant eu des accidents mortels pour adapter les conditions de ses polices d'assurance.
[358] Sur l'importance du principe de minimisation, v. *infra*, n^os^ 446 s.
[359] C. Pérès, « Les données à caractère personnel et la mort. Observations relatives au projet de loi pour une République numérique », *D.* 2016, p. 90, n° 12.

mort[360]. Aujourd'hui, le droit reconnaît à la personne décédée une sorte de *continuum*, qui se matérialise par une protection « résiduelle »[361]. Pour s'en convaincre, il suffit de s'intéresser aux récentes modifications législatives liées à la protection du corps humain. Par exemple, le droit au respect du corps humain vivant[362] a été étendu au profit du corps mort[363], par l'introduction d'un article 16-1-1 du code civil[364]. Celui-ci reconnaît que « le respect dû au corps humain ne cesse pas avec la mort. Les restes des personnes décédées, y compris les cendres de celles dont le corps a donné lieu à crémation, doivent être traités avec respect, dignité et décence »[365]. Le code pénal sanctionne, dans son article 225-17, l'atteinte à la sépulture ou à l'intégrité du cadavre. Même en matière de droit moral de l'auteur, quelques brèches à la séparation binaire entre la personne vivante et la personne morte sont à relever[366].

La protection *post mortem* des données personnelles s'inscrit donc dans cette conception renouvelée de la personne. Pour autant, ce rapprochement doit être nuancé. En effet, la reconnaissance des droits *post mortem* sur les données personnelles semble avoir été justifiée par les difficultés pratiques rencontrées par les ayants-droit d'une personne décédée[367]. Il était fréquent que leur action se heurte à d'importantes difficultés lors de l'accès aux données du défunt. Le droit au respect du corps humain est plutôt fondé sur l'objectif de protection de l'être humain[368].

101. Des limites pratiques à l'effectivité de la protection *post mortem*. Plusieurs difficultés entravent l'exercice des droits *post mortem* par les ayants-droit[369]. Tout d'abord, un recensement exhaustif des données personnelles s'avère, en pratique,

---

[360] Pour un aperçu historique des contours de l'existence de la personne physique, v. J. Carbonnier, *Droit civil,* vol. 1, *Introduction. Les personnes. La famille, l'enfant, le couple*, PUF, 2004, n° 207, p. 400.
[361] J. Rochfeld, *Les grandes notions du droit privé,* 2e éd., PUF, 2013, *V°* « La personne », n° 12, p. 32.
[362] Art. 16-1 du code civil.
[363] L'article 11 de la loi n° 2008-1350 du 19 décembre 2008 a introduit ce nouvel article dans le code civil. Pour une analyse critique de cette loi, v. F. Terré et D. Fenouillet, *Droit civil. Les personnes*, 8e éd., Dalloz, 2012, n° 55, p. 61.
[364] La portée de cette reconnaissance doit être atténuée étant donné que ce principe préexistait à l'adoption de la loi, v. D. Mainguy, « À propos d'un "principe" préexistant à une loi », *D.* 2015, p. 246.
[365] Pour une analyse de cet article, v. not. *JCl. civil code,* art. 16 à 16-4, fasc. 72, « Respect et protection du corps humain. Le mort », par B. Beignier et Y. Puyo, 2013 (actu. 2017), nos 8 s. ; G. Loiseau, « *Mortuorum corpus* : une loi pour le respect », *D.* 2009, p. 236.
[366] V. not. pour la dévolution des droits moraux de l'auteur, v. C. Caron, *Droit d'auteur et droits voisins*, 5e éd., LexisNexis, 2017, nos 276 s.
[367] V. Gouvernement, Étude d'impact pour le projet de loi pour une République numérique, 9 déc. 2015, p. 109 s.
[368] V. not. G. Loiseau, « *Mortuorum corpus* : une loi pour le respect », *D.* 2009, p. 236 ; B. Edelman, « Entre le corps – objet profane – et le cadavre – objet sacré », *D.* 2010, p. 2754 ; M. Bacache, « Corps humain. Têtes maories », *RTD civ.* 2010, p. 626 ; P.-J. Delage, « Respect des morts, dignité des vivants », *D.* 2010, p. 2044.
[369] Pour une analyse du régime du maintien provisoire de l'exercice de certains droits sur les données personnelles du *de cujus,* F. Bicheron, « La mort numérique », in *Mélanges M. Grimaldi*, Defrénois, 2020, p. 81 s., n° 13, spéc. p. 87.

pratiquement impossible. À la difficulté d'établir la liste de tous les services auxquels le *de cujus* est conscient d'avoir confié ses données[370], s'ajoute la tâche quasiment impossible de dénombrer les services ayant enregistré les informations à son insu. En effet, la qualification de données à caractère personnel ne se limite pas aux seules données que la personne a conscience d'avoir fournies, mais s'étend également aux données générées par son activité (numérique ou non), ou inférées à partir de ses données ou de son activité[371].

À ces difficultés de recensement s'ajoutent également les problèmes liés à la mise en œuvre de ces droits. Déjà au sujet du droit à la suppression des données[372], certains problèmes dans l'effacement des données ont été détectés. Par exemple, en 2011, Monsieur Maximilian Schrems avait dénoncé la pratique de Facebook consistant à effacer les données uniquement du côté de l'utilisateur, et à les conserver dans les systèmes d'information de l'entreprise[373]. Seule la personne vivante particulièrement attentive peut éventuellement se rendre compte d'une telle pratique. Les héritiers seront dans l'impossibilité de vérifier l'intégralité de l'effacement et devront faire confiance aux responsables du traitement.

D'autres questions pratiques sont soulevées à l'occasion de la mise en œuvre de ces dispositions. Par exemple, lorsqu'une personne décède, n'existerait-il pas, pour le responsable du traitement, un intérêt légitime à la conservation des données dans son système d'information ? Et ce, particulièrement lorsque le système génère de nouvelles données à partir de celles fournies par l'utilisateur, comme c'est le cas notamment des algorithmes d'intelligence artificielle[374]. Une obligation d'effacement intégral de ces données risque d'engendrer des conséquences disproportionnées pour le responsable du traitement en comparaison de l'atteinte à la personne résultant de ces traitements.

---

[370] Sur la difficulté de faire l'inventaire des sites sur lesquels une personne s'est inscrite, A. Léchenet, « Comment j'ai commencé à disparaître de l'Internet », *Libération* 16 oct. 2016.

[371] Classiquement, il existe trois types de données à caractère personnel : les données « produites » par la personne, les données « générées » par son activité et les données « dérivées ou inférées » à partir des données fournies par cette personne ou son activité. Sur cette distinction v. F. Georges, « Représentation de soi et identité numérique. Une approche sémiotique et quantitative de l'emprise culture du web 2.0 », *Réseaux* 2009, nº 154, p. 165 ; v. également H. Guillaud, « Les trois niveaux de nos identités en ligne », *InternetActu* 2 févr. 2019. Dans sa délibération du 21 janvier 2019, la CNIL reprend aussi cette distinction, délibération nº 2019-001 du 21 janv. 2019 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google LLC, § 108.

[372] Le droit à l'effacement est au cœur du dispositif de protection des données des personnes décédées.

[373] M. Schrems, « Complaint against Facebook Ireland Ltd. », *europe-v-facebook.org* 18 août 2011. Un jugement du tribunal de grande instance de Paris a confirmé l'existence de cette pratique, v. TGI Paris, 9 avr. 2019, *UFC-Que Choisir* c. *Facebook*, nº 14/07928, p. 37.

[374] Sur l'articulation entre le droit à l'effacement des données et l'éventuel intérêt du responsable du traitement, v. *infra,* nº 374.

Par ailleurs, les tiers ayant eu accès aux données du *de cujus* après son décès et avant une demande d'effacement des héritiers, doivent-il être contraints par le respect des règles du droit des données personnelles ? La réponse doit sans doute être négative puisqu'à partir du décès de la personne, ses données ne sont plus couvertes par la notion. Ces questions ne trouvent pas vraiment de réponses en droit positif et encouragent donc à s'interroger sur la portée véritable des droits reconnus par la loi d'octobre 2016.

En tout état de cause, cette reconnaissance étend, au moins partiellement, certaines protections juridiques issues du droit des données à caractère personnel au bénéfice de personnes décédées. Elle apporte donc une nuance à l'acceptation civiliste classique de la notion de personne physique selon laquelle la personnalité juridique, et donc la capacité d'être sujet de droits, s'éteint au décès de la personne.

3. Les données permettant d'obtenir des informations sur une personne vivante

102. Les données, témoins des liens entre les personnes. Dans certains cas, des données relatives à une personne à naître ou à une personne décédée peuvent entretenir un lien avec une personne vivante. C'est le cas de certaines données de santé, particulièrement les données génétiques qui offrent des informations non seulement sur la personne concernée mais également sur son entourage familial[375]. L'arrêt de la cour d'appel de Paris relatif au cadavre d'Yves Montand illustre bien le rapport pouvant exister entre un cadavre et une personne vivante. Dans cette affaire particulièrement médiatisée, la cour d'appel avait ordonné de faire exhumer le corps d'Yves Montand pour vérifier son éventuelle paternité à l'égard de Madame Aurore Drossart[376]. En effet, les héritiers d'Yves Montand avaient demandé à faire réaliser une analyse ADN sur son cadavre[377]. C'est parce que les informations d'une personne décédée (ici Yves Montand) peuvent renseigner sur une personne vivante (en l'espèce Aurore Drossart) que cette demande avait été faite.

---

[375] L'article 4 de la déclaration internationale sur les données génétiques de l'UNESCO du 16 octobre 2003 reconnaît que l'une des spécificités de ces données tient au fait « qu'elles peuvent avoir une incidence significative sur la famille, y compris la descendance, sur plusieurs générations, et dans certains cas sur l'ensemble du groupe auquel appartient la personne concernée ». G. Cornu, *Droit civil. Les personnes*, 13e éd., Montchrestien, 2007, nº 19, p. 39. Sur la génétique mobilisée à des fins d'identification dans le procès pénal, v. E. Supiot (dir.), « Le procès pénal à l'épreuve de la génétique », Rapport Mission de recherche droit et justice, 2017, p. 95 s.

[376] CA Paris, 6 nov. 1997, nº 94/27539, *D.* 1998, p. 122.

[377] Les héritiers avaient fait cette demande alors même qu'Yves Montand avait continuellement refusé de s'y soumettre de son vivant.

Les exemples de données pouvant entretenir un lien avec une personne vivante pourraient être multipliés. Il en va ainsi notamment du séquençage génétique de l'ADN. Celui-ci permet d'obtenir des informations tant sur la mère (notamment avec le chromosome Y) que sur l'enfant (le mélange unique avec les gênes du père). Si une mère décède en laissant derrière elle une fille, l'étude de l'ADN du chromosome Y de la mère correspond, à quelques mutations près, à celui de sa fille.

Les données d'une personne à naître ou décédée peuvent apporter des informations sur une personne vivante. Elles doivent donc être protégées sur le fondement du droit des données à caractère personnel, alors même qu'elles ne concernent pas une personne physique au sens strict. En effet, ces données peuvent être prélevées sur un embryon ou un cadavre, lesquels ne sont pas considérés comme une personne physique au sens traditionnel du droit civil.

En plus de cette extension des contours de la notion de personne physique, il apparaît, de manière plus surprenante, que certaines personnes morales réussissent aussi à se glisser dans la notion de personne physique au sens du droit des données à caractère personnel.

B. Une exclusion relative des personnes morales

103. Définition de la personne morale. Classiquement, la personne morale est définie comme un groupement doté, sous certaines conditions, d'une personnalité juridique[378]. Elle a donc tous les attributs de la personnalité juridique : un nom (appelé dénomination ou raison sociale pour les sociétés), un domicile (un siège social), un patrimoine, une nationalité, la capacité juridique (par exemple de conclure des contrats), etc.[379]. Dès lors que la personne morale a une personnalité juridique, il a rapidement été question de savoir si elle bénéficiait des mêmes attributs de la personnalité que la personne physique.

104. Les droits de la personnalité et les personnes morales. C'est d'abord au sujet de la reconnaissance des droits de la personnalité au bénéfice des personnes morales que les réflexions doctrinales se sont orientées[380]. Dans son emblématique étude sur le

---

[378] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *V°* « Personne », spéc. morale.
[379] M. Fabre-Magnan et F. Brunet, *Introduction générale au droit,* PUF, 2017, n° 180, p. 241.
[380] En éclaireur, Ripert avait pressenti « la grande habileté » du capitalisme libéral à considérer la personnalité des êtres moraux comme semblable à celle des êtres humains et à revendiquer, pour les personnes morales, la jouissance des mêmes droits que ceux des personnes humaines, v. G. Ripert, *Aspects juridiques du capitalisme moderne*, 2e éd., LGDJ, 1955, n° 30, p. 74.

sujet, Pierre Kayser affirmait que les personnes morales sont investies de « droits analogues aux droits de la personnalité. Elles sont seulement privées de ceux de ces droits dont l'existence a un lien nécessaire avec la personnalité humaine »[381]. Ainsi, la doctrine et la jurisprudence ont rapidement reconnu aux personnes morales une protection juridique de leur nom[382], de leur honneur[383] ou de leur domicile[384].

Quant à la reconnaissance d'un éventuel droit au respect de leur vie privée, deux courants doctrinaux s'opposent[385]. D'un côté, certains auteurs se montrent défavorables à son extension au bénéfice des personnes morales, en considérant que celles-ci ne peuvent avoir une vie privée, au sens propre de cette expression[386]. De l'autre, quelques auteurs accueillent plutôt favorablement cette reconnaissance[387]. Après un timide élan jurisprudentiel reconnaissant aux personnes morales le bénéfice du droit au respect de la vie privée[388], la Cour de cassation a finalement déclaré que « si les personnes morales disposent, notamment, d'un droit à la protection de leur nom, de leur domicile, de leurs correspondances et de leur réputation, seules les personnes physiques peuvent se prévaloir d'une atteinte à la vie privée au sens de l'article 9 du code civil »[389]. Ainsi, il

---

[381] P. Kayser, « Les droits de la personnalité. Aspects théoriques et pratiques », *RTD civ.* 1971, p. 445, n° 39. V. aussi, G. Cornu, *Droit civil. Les personnes*, 13e éd., Montchrestien, 2007, nos 99 s., p. 219 s.

[382] M. Dagot, « Le nom des personnes morales », *JCP G* 1992, I, doctr. 3579. Sur la protection du nom commercial, v. *Rép. com.* Dalloz, *Vo* « Nom commercial », par G. Loiseau, 2002 (actu. 2011), nos 57 s. En ce sens, la Cour de cassation reconnaît aux personnes morales un droit au nom, v. not. Cass. civ. 1re, 5 déc. 1966, *Bull. civ.* 1966, n° 534 ; Cass. civ. 1re, 8 nov. 1988, n° 86-13.264, *Bull. civ.* 1988, n° 312, p. 212.

[383] B. Beignier, *L'honneur et le droit*, th. Paris II, 1995, LGDJ, p. 244 s. La Cour de cassation reconnaît aux personnes morales le bénéfice du droit à l'honneur ou à la réputation, Cass. crim., 12 oct. 1976, n° 75-90.239, *Bull. civ.* 2006, n° 273, p. 238.

[384] La Cour de cassation a affirmé le principe de protection du domicile des personnes morales en 1995, v. Cass. crim., 23 mai 1995, n° 94-81.141, *Bull. crim.* 1995, n° 193, p. 524. La question de la protection du domicile des personnes morales a été portée devant la CEDH qui a considéré, dans un arrêt de 2002, que le siège social de la personne morale est protégé comme le domicile d'une personne physique, v. CEDH, 16 avr. 2002, *Colas Est et autres* c. *France*, n° 37971/97, § 51. Pour une analyse de cette décision, v. not. C. Bîrsan, « La notion de domicile au sens de l'article 8 de la Convention vise le siège social, les agences et les locaux professionnels d'une personne morale », *D.* 2003, p. 527. La Cour de justice retient une interprétation similaire, v. not. CJCE, 22 oct. 2002, *SA Roquette Frères* c. *Directeur général de la concurrence, de la consommation et de la répression des fraudes*, C-94/00, § 29. Pour un bref exposé de cette reconnaissance, v. J. Rochfeld, *Les grandes notions du droit privé,* 2e éd., PUF, 2013, *Vo* « Les groupements de personnes », n° 8, p. 88.

[385] Pour une étude des courants doctrinaux relatifs aux droits de la personnalité, v. *Rép. civ.* Dalloz, *Vo* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), nos 165 s.

[386] P. Kayser, « Les droits de la personnalité. Aspects théoriques et pratiques », *RTD civ.* 1971, p. 445, n° 39 ; N. Mathey, « Les droits et libertés fondamentaux des personnes morales de droit privé », *RTD civ.* 2008, p. 205. Plus largement au sujet des déviances liées à la reconnaissance de droits de la personnalité aux personnes morales, v. G. Loiseau, « Des droits humains pour personnes non humaines », *D.* 2011, p. 2558.

[387] F. Petit, « Les droits de la personnalité confrontés au particularisme des personnes morales », *Dalloz Affaires* 1998, p. 826 ; L. Dumoulin, « Les droits de la personnalité des personnes morales », *Revue des sociétés* 2006, p. 1, n° 12 et n° 24.

[388] C'est un arrêt de la cour d'appel d'Aix-en-Provence affirmant que « les personnes morales sont susceptibles de subir une atteinte à leur vie privée » qui leur a reconnu le bénéfice de cette protection, CA Aix-en-Provence, 1re ch., 10 mai 2001, n° 10/052001, *D.* 2002, p. 2299.

[389] Cass. civ. 1re, 17 mars 2016, n° 15-14.072, *Bull. civ.* 2016, I, n° 1060. Au contraire, la CEDH accepte de reconnaître aux personnes morales le bénéfice d'une protection de leur vie privée, v. not. CEDH, 16 décembre 1992, *Niemietz* c. *Allemagne*, n° 13710/88, § 31 ; CEDH, 16 avr. 2002, *Colas Est et autres* c. *France*, n° 37971/97, § 51. Pour une analyse de ces interprétations, v. not. F. Sudre, « Article II-67 », in *Traité établissant une Constitution pour l'Europe, commentaire article par article. Partie 2 : La Charte des droits fondamentaux*, t. 2,

apparaît que les personnes morales ne peuvent pas bénéficier du droit au respect de la vie privée. Cette exclusion se retrouve aussi en droit des données à caractère personnel.

105. Une exclusion de principe des personnes morales de la notion de donnée à caractère personnel. En visant les personnes physiques dans la définition de la donnée à caractère personnel, les législateurs français et européen excluent *de facto* les personnes morales. Une telle exclusion est d'ailleurs explicitement confirmée par le considérant 14 du règlement européen, lequel affirme que ce texte « ne couvre pas le traitement des données à caractère personnel qui concernent les personnes morales ».

Déjà en 1977, les parlementaires français avaient écarté les personnes morales du champ d'application de la loi Informatique et libertés, en justifiant cette exclusion par le fait que ces dispositions avaient pour but de « protéger les droits de la personne, sa vie privée et son intimité »[390]. Dès lors, par principe, les données se rapportant à des personnes morales ne sont pas qualifiées comme des données à caractère personnel. Ce principe trouve toutefois quelques tempéraments.

106. Une reconnaissance nationale possible. Si la plupart des textes relatifs aux données à caractère personnel excluent les personnes morales de leur champ d'application, la Convention 108 du Conseil de l'Europe[391] autorise les États signataires à inclure ces personnes dans le domaine de la notion de donnée à caractère personnel[392]. Seuls l'Autriche, le Danemark, le Luxembourg, l'Italie et la Suisse[393] ont reconnu aux

---

dir. L. Burgorgue-Larsen, A. Levade et F. Picod, Bruylant, 2005, nº 14. La CEDH rappelle quand même que l'atteinte à la réputation d'une personne physique et d'une société n'ont pas la même nature et les mêmes conséquences, v. CEDH, 19 juill. 2011, *UJ* c. *Hongrie*, nº 23954/10, § 22. Quant à la Cour de justice, elle considère également que la notion de vie privée ne saurait être interprétée comme « excluant les activités professionnelles ou commerciales des personnes physiques comme des personnes morales », v. CJCE, 14 févr. 2008, *Varec SA* c. *État belge*, C-450/06, § 48.

[390] J. Foyer, « Rapport sur le projet de loi modifié par le Sénat relative à l'informatique et aux fichiers », Assemblée nationale, nº 3352, t. 1, 14 déc. 1977, p. 3. Les parlementaires de 1978 avaient évoqué l'éventualité d'une reconnaissance aux personnes morales sans but lucratif d'un droit sur leurs informations nominatives, v. not. J. Thyraud, « Rapport sur le projet de loi, adopté par l'Assemblée nationale, relatif à l'informatique et aux libertés », Sénat, nº 72, 10 nov. 1977, p. 23. Sur l'exclusion initiale des personnes morales de la loi Informatique et libertés, v. P. Ancel, « La protection des données personnelles : aspects de droit privé français », *RID comp.* 1987, vol. 39, nº 3, p. 609, spéc. p. 624.

[391] Conseil de l'Europe, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* nº 108, 28 janv. 1981 (dite Convention 108).

[392] Art. 3 § 2 (b) de la Convention nº 108.

[393] En Suisse, par exemple, c'est pour des raisons de cohérence que la protection des personnes morales est reconnue par le droit des données personnelles. En effet, le code civil leur accorde une protection sur le fondement des droits de la personnalité. Ainsi, lorsqu'il a été question d'étendre le bénéfice du droit des données personnelles aux personnes morales, le Conseil fédéral suisse a considéré que refuser de reconnaître aux personnes morales le bénéfice de la protection de ce droit « romprait avec la tradition juridique suisse ». Par ailleurs, le Conseil fédéral considérait que cette protection existerait *de facto* à l'égard des petites entreprises qui sont souvent en relation étroite avec les personnes physiques, v. Conseil fédéral suisse, « Message concernant la loi fédérale sur la protection des données (LPD) », 23 mars 1988, *Feuille fédérale,* 140e année, vol. 2, p. 421 s., spéc. p. 447.

personnes morales une protection de leurs données sur le fondement du droit des données personnelles[394]. Une fragmentation de la notion est donc à déplorer sur ce sujet sur le territoire européen. Toutefois, même lorsque le législateur n'a pas expressément reconnu le bénéfice des dispositions du droit des données à caractère personnel aux personnes morales, celles-ci réussissent tout de même à instrumentaliser cette protection à leur bénéfice.

107. Une reconnaissance possible de la protection des données personnelles au bénéfice des personnes morales. Même lorsque les textes ont fermement écarté les personnes morales de la notion de donnée à caractère personnel, des tempéraments à ce principe sont à déplorer. Tout d'abord, il a été considéré que les liens entretenus par la personne morale avec une personne physique peuvent être d'une nature telle que celle-ci peut bénéficier de la protection de ses données. C'est notamment le cas lorsque le nom de la personne morale est attaché à celui d'une personne physique[395]. Ainsi, la Cour de justice de l'Union européenne a considéré que les personnes morales bénéficiaires d'aides peuvent se prévaloir des droits reconnus aux articles 7 et 8 de la Charte de l'Union européenne dans la mesure où leur nom légal identifie une ou plusieurs personnes physiques[396]. En adoptant un raisonnement similaire, la CNIL a considéré que les informations d'une personne morale liées à une personne physique, notamment celles présentes dans le registre des sociétés[397], doivent faire l'objet d'un traitement particulier[398]. Si, en 2002, le Conseil d'État avait initialement rejeté une telle

---

[394] N. Campagne, « La protection "informatique et libertés" des données des personnes morales en Europe », *RLDI* 2014, n° 104, p. 62 et G29, WP 136, Avis 4/2007 du groupe de travail relatif au concept de données à caractère personnel, 20 juin 2007, p. 26.

[395] Sur l'utilisation du nom d'une personne physique par une personne morale, v. G. Loiseau, *Le nom, objet d'un contrat*, th. Paris I, 1995, LGDJ, n^os^ 185 s., p. 193 s. V. aussi, *Rép. civ.* Dalloz, *V^o^* « Nom – Prénom », par F. Laroche-Gisserot, 2014 (actu. 2019), n^os^ 432 s. ; M. Vivant, « Le patronyme saisi par le patrimoine », in *Mélanges A. Colomer*, Litec, 1993, p. 517 s., n° 14, spéc. p. 526.

[396] CJUE, 9 nov. 2010, *Volker und Markus Schecke GbR* et *Hartmut Eifert* c. *Land Hessen*, C-92/09 et C-93/09, § 53. Cette reconnaissance doit être critiquée puisque la Cour permet de contourner facilement les dispositions visant à garantir une meilleure transparence dans l'attribution des fonds européens. Pour cela, la personne morale doit simplement entretenir des liens suffisants avec une personne physique et elle pourra échapper à la transparence pourtant souhaitée par le législateur.

[397] Il s'agit par exemple des informations relatives à un dirigeant de société, à un entrepreneur individuel ou à une profession libérale. L'obligation d'inscription est encadrée par les articles L. 123-1 s. du code de commerce.

[398] CNIL, « Un site peut-il réutiliser les informations du Registre du commerce et des sociétés ? ». La Cour de justice de l'Union européenne s'est également prononcée sur ce sujet en considérant que « la circonstance que ces informations s'inscrivent dans le contexte d'une activité professionnelle n'est pas de nature à leur ôter la qualification de données à caractère personnel », v. CJUE, 9 mars 2017, *Camera di comercio* c. *Salvatore Manni*, C-398/15, § 34. Comp. les données personnelles des bénéficiaires effectifs de sociétés, A. Rocher, « Les données personnelles des bénéficiaires effectifs de sociétés », *Revue des Sociétés* 2020, p. 139. La Cour de cassation a également, dans une récente décision, considérée que l'atteinte à la protection des données personnelles d'un associé était proportionnée au but légitime de détection et de prévention des difficultés des entreprises dès lors que « les comptes annuels d'une société par actions simplifiée unipersonnelle ne constituent (…) qu'un des éléments nécessaires à la détermination de la valeur des actions que possède son associé unique, dont le

interprétation en considérant que « les entrepreneurs individuels, pris en cette qualité, ne sont pas des personnes physiques pour l'application » des dispositions du 6 janvier 1978[399], cette conception ne paraît plus possible aujourd'hui, compte tenu de l'extension de la notion de donnée à caractère personnel et de l'interprétation retenue par la Cour de justice de l'Union européenne[400].

Enfin, la directive vie privée et communications électroniques, pourtant relative au traitement des données à caractère personnel et à la protection de la vie privée, étend aux personnes morales le bénéfice de quelques-unes de ses dispositions[401]. En effet, les fournisseurs du service sont tenus de les informer des types de données qu'ils traitent, des finalités des traitements et de leurs durées[402].

Dans ces hypothèses, la personne morale réussit à se glisser dans la notion de personne physique au sens du droit des données à caractère personnel, écartant donc une interprétation stricte de cette notion. Une telle extension n'est pas exempte de critiques.

108. Critiques quant à l'inclusion des personnes morales dans la notion de donnée à caractère personnel. L'extension de la notion de donnée à caractère personnel aux personnes morales, particulièrement celles à but lucratif, apparaît inadaptée et injustifiée. Inadaptée puisque l'objectif de cette protection a toujours été de garantir aux êtres humains le respect de leur identité, de leur vie privée, ainsi que de leur autonomie personnelle[403]. Cette protection est superflue pour les personnes morales précisément parce que celles-ci étant une abstraction, elles n'ont pas besoin d'espaces d'intimité pour se développer librement.

---

patrimoine, distinct de celui de la société, n'est qu'indirectement et partiellement révélé », Cass. com., 24 juin 2020, nº 19-14.098, *Bull. com.* 2020.

[399] CE Sec., 3 juill. 2002, *Ministre de l'équipement, des transports et du logement* c. *Association française de l'apprentissage de la conduite (AFAC)*, nº 157402, *Lebon T.* p. 730.

[400] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 601, p. 256.

[401] Directive CE nº 2002/58 du Parlement européen et du Conseil du 12 juill. 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *JOCE* 31 juill. 2002, L-201, p. 37 s. Monsieur Grégoire Loiseau n'a pas manqué de critiquer l'extension du bénéfice des règles relatives à la protection des données personnelles à l'égard des personnelles morales, v. G. Loiseau, « Des droits humains pour personnes non humaines », *D.* 2011, p. 2558. Madame Céline Castets-Renard note également que cette directive ne retenait pas « la conception étroite de la directive 95/46/CE consistant à protéger les données personnelles des seules personnes physiques », *Rép. eur.* Dalloz, *Vº* « La protection des données personnelles dans les relations internes à l'Union européenne », par C. Castets-Renard, 2018 (actu. 2020), nº 265.

[402] Cons. 12, cons. 26 et art. 6 de la directive CE nº 2002/58.

[403] Sur les types d'atteintes aux personnes auxquels le droit des données à caractère personnel doit répondre, v. *infra*, nº 377. Sur les déviances liées à la reconnaissance de droits de la personnalité aux personnes morales, v. not. G. Loiseau, « Des droits humains pour personnes non humaines », *D.* 2011, p. 2558.

Pourtant, les personnes morales n'hésitent pas à instrumentaliser le droit des données à caractère personnel à leur propre avantage. Par exemple, Facebook a saisi la Cour de justice de l'Union européenne pour contester les demandes effectuées par la Commission européenne dans le cadre de son enquête sur les éventuelles pratiques anticoncurrentielles de l'entreprise[404]. La Commission a notamment demandé à l'entreprise de lui fournir les documents contenant des mots ou expression (« big question », « for free », ou « shutdown »), mots considérés par Facebook comme trop larges et attentatoires à la protection des données à caractère personnel de ses employés.

Par ailleurs, cette extension est injustifiée parce que les personnes morales bénéficient de fondements spécialement conçus pour elles, leur garantissant déjà des droits sur leurs données[405]. Par exemple, le secret des affaires protège les informations qui revêtent « une valeur commerciale, effective ou potentielle »[406]. Ce secret leur garantit une protection contre la divulgation de ces informations et sanctionne les investigations indiscrètes de la part des tiers[407]. À cette protection déjà très large s'ajoutent de nombreuses règles sectorielles protégeant les données des entreprises[408], telles que l'ensemble des droits reconnus par le droit de la propriété intellectuelle[409], ou les dispositions du droit de la concurrence relatives au dénigrement[410].

---

[404] F. Yun Chee, « Facebook gains temporary court reprieve on EU antitrust data demand », *Reuters* 28 juill. 2020.
[405] Pour un panorama des protections juridiques de l'information reconnues par le droit au bénéfice des personnes morales, v. M. Malaurie-Vignal, « Réflexions sur la protection du patrimoine informationnel de l'entreprise contre le piratage économique », *D.* 2012, p. 1415. Pour une comparaison entre les données personnelles et économiques, v. B. Gauriau et A. Teissier, « Données personnelles et économiques : l'interdiction de diffuser », *JCP S* 2020, n^{os} 20 s., p. 2028 s.
[406] V. directive UE n^{o} 2016/943du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, *JOUE* 15 juin 2016, L-157/1, p. 1 s. Cette directive a été transposée en droit français par la loi n^{o} 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires, *JORF* 31 juill. 2018, n^{o} 0174, texte 1. Désormais l'article L. 151-1 du code de commerce protège, au titre du secret des affaires, « toute information répondant aux critères suivants : 1° Elle n'est pas, en elle-même ou dans la configuration et l'assemblage exacts de ses éléments, généralement connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur secteur d'activité ; 2° Elle revêt une valeur commerciale, effective ou potentielle, du fait de son caractère secret ; 3° Elle fait l'objet de la part de son détenteur légitime de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret ». Sur la directive, v. not. J.-C. Galloux, « L'adoption de la directive sur les secrets d'affaires », *RTD com.* 2017, p. 59. Pour une critique du champ d'application de ce secret, v. J.-C. Roda, « Secret des affaires : et si l'on avait manqué l'essentiel ? », *D.* 2018, p. 1318. Sur les incertitudes ajoutées par le législateur français lors de la transposition de cette directive, v. M. Dhenne, « La loi n^{o} 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires », *D.* 2018, p. 1817.
[407] V. déjà en ce sens, C. Gavalda, « Le secret des affaires », in *Mélanges R. Savatier*, Dalloz, 1965, p. 291 s.
[408] Sur la juxtaposition avec les autres régimes de protection profitant aux personnes morales, v. L. Dumoulin, « Les droits de la personnalité des personnes morales », *Revue des sociétés* 2006, p. 1 s., n^{os} 21 s.
[409] V. par ex. le droit reconnu sur les bases de données, N. Binctin, *Droit de la propriété intellectuelle. Droit d'auteur, brevet, droits voisins, marque, dessins et modèles,* 6^{e} éd., LGDJ, 2020, p. 231 s., ou les droits reconnus en matière d'œuvres collectives, v. A. Lucas, A. Lucas-Schloetter et C. Bernault, *Traité de la propriété littéraire et artistique*, 5^{e} éd., LexisNexis, 2017, n^{os} 216 s., p. 234 s.
[410] Le dénigrement, tel que défini par Paul Roubier, vise les agissements qui « tendent à jeter le discrédit sur un concurrent ou sur les produits fabriqués », P. Roubier, *Le droit de la propriété industrielle*, t. 1, Sirey, 1952,

Pour résumer, même si les personnes morales n'entrent pas *a priori* dans le domaine de la notion de donnée à caractère personnel, elles réussissent tout de même à s'y glisser. Cette extension aux personnes morales a tendance à faire oublier l'objectif initial du droit des données à caractère personnel. Celui-ci visait à garantir le développement d'une informatique respectueuse des libertés individuelles.

La variation des degrés du rattachement entre la donnée et la personne témoignent également du caractère large de la notion de donnée à caractère personnel.

§ II. Les degrés du rattachement entre la donnée et la personne

109. L'identification. La qualification de donnée à caractère personnel s'applique aux données *se rapportant* à une personne physique. Le législateur a choisi une conception large du lien puisque la donnée doit « se rapporter » à une personne. Pour déterminer si une donnée se rapporte à un individu, c'est-à-dire si elle se rattache à une personne[411], il faut étudier le *potentiel identifiant* de cette donnée[412]. Ainsi, ce sont toutes les informations participant au processus d'identification, même lorsque cette identification n'est qu'éventuelle, qui sont couvertes par la notion de donnée à caractère personnel[413].

110. Plan. L'identification renvoie à l'action d'identifier, c'est-à-dire à la capacité de « faire connaître à autrui, au sein d'une gamme de choses particulières du même type, celle [la personne] dont nous avons l'intention de parler »[414]. Pour qu'une donnée soit considérée comme une donnée à caractère personnel, il faut qu'elle identifie directement (A) ou indirectement (B) une personne. Seuls l'absence complète de

p. 506. Sur les moyens du dénigrement, v. *Rép. com.* Dalloz, *V°* « Concurrence déloyale », par Y. Picod, Y. Auguet et N. Dorandeu, 2010 (actu. 2020), n^os^ 154 s.

411 *Dictionnaire de l'Académie française*, 9e éd., *V°* « Rapporter », sens IV.

412 A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, n° 496, p. 220.

413 En 1978, le législateur français avait défini les informations nominatives comme « 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 », art. 4 de la loi n° 78-17 du 6 janv. 1978. Pour une étude de cette notion, v. *infra*, n^os^ 138 s.

414 P. Ricœur, *Soi-même comme un autre*, Seuil, 1996, p. 39. V. aussi A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, n° 505, p. 222. Pour Madame Astrid Marais, « identifier une personne, c'est dégager les éléments qui permettent de cerner son identité afin de l'individualiser dans la société en la distinguant des autres ». Ainsi, l'identification est intrinsèquement liée à l'identité (et à ses composantes), A. Marais, *Droits des personnes*, 3e éd., Dalloz, 2018, n° 123, p. 87.

rattachement ou le rattachement impossible avec une personne privent la donnée de cette qualification (C).

A. L'identification directe de la personne

111. Les types d'informations permettant un rattachement direct. Deux types d'informations rendent possible un rattachement *direct* entre une donnée et une personne physique : il s'agit, d'une part des informations directement identifiantes, et d'autre part des informations concernant une personne physique identifiée.

112. L'information directement identifiante. Le droit a assigné à certaines informations la fonction d'identifier la personne[415]. Parmi celles-ci figurent incontestablement les données relatives à l'état des personnes[416]. Ce dernier est classiquement défini comme l'ensemble des caractères biologiques et sociaux permettant d'individualiser une personne dans la société dans laquelle elle vit[417]. Dresser une liste exhaustive des éléments qui relèvent de l'état des personnes représenterait un exercice fastidieux[418], mais il est certain que sont inclus dans cette notion les éléments caractérisant la situation juridique d'une personne au plan individuel (date et lieu de naissance, nom, prénom, sexe, capacité, domicile), au plan familial (filiation, mariage, pacs) et au plan politique (qualité de Français ou d'étranger)[419]. Pour ces informations, la donnée et l'identité de la personne se confondent ; plus précisément, les *informations caractérisent la personne*[420]. Elles lui sont par nature liées et entrent évidemment dans la définition de donnée à caractère personnel.

---

[415] La question de l'identité a fait l'objet de riches travaux doctrinaux, v. par ex. D. Gutmann, *Le sentiment d'identité. Étude de droit des personnes et de la famille*, th. Paris II, 2000, LGDJ ; J. Pousson-Petit (dir.), *L'identité de la personne humaine : étude de droit français et de droit comparé*, Bruylant, 2003 ; V. Sagné, *L'identité de la personne humaine,* th. Toulouse I, 2003.

[416] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vo* « État (I) », sens 1 ; v. aussi, A.-M. Leroyer, « La notion d'état des personnes », in *Mélanges M. Gobert*, Economica, 2004, p. 247 s., no 1, spéc. p. 247.

[417] F. Zenati-Castaing et T. Revet, *Manuel de droit des personnes*, PUF, 2006, no 33, p. 49.

[418] J. Rochfeld, *Les grandes notions du droit privé,* 2e éd., PUF, 2013, *Vo* « La personne », no 16, p. 39.

[419] *Rép. civ.* Dalloz, *Vo* « État et capacité des personnes – État », par I. Gallmeister, 2016 (actu. 2019), no 4 ; G. Cornu, *Droit civil. Les personnes*, 13e éd., Montchrestien, 2007, nos 37 s., p. 83 s. ; J. Carbonnier, *Droit civil,* vol. 1, *Introduction. Les personnes. La famille, l'enfant, le couple*, PUF, 2004, no 74, p. 131. Monsieur Bernard Teyssié distingue trois catégories au sein du « statut civil de l'être humain » : le statut individuel, le statut familial et le statut social, v. B. Teyssié, *Droit des personnes*, 21e éd., LexisNexis, 2019, no 13, p. 13.

[420] Selon Madame Judith Rochfeld, le « modèle issu du code civil fait la part belle à une "identité régalienne", c'est-à-dire placée au service de l'État et remplissant une fonction d'identification », v. J. Rochfeld, « La vie tracée ou le code civil doit-il protéger la présence numérique des personnes ? », in *Mélanges J. Hauser*, LexisNexis et Dalloz, 2012, p. 619 s., no 6, spéc. p. 624.

113. L'information concernant une personne physique identifiée. En ajoutant une référence aux données concernant une personne physique identifiée, la directive de 1995 a introduit en droit français une nouvelle catégorie de données personnelles. Avant cette date, l'article 4 de la loi du 6 janvier 1978 distinguait seulement entre les informations permettant l'identification directe et celles permettant l'identification indirecte. L'ajout dans la définition des informations « concernant une personne physique identifiée » a étendu le champ d'application de la notion de donnée à caractère personnel, d'autant que les législateurs n'ont pas assorti cette catégorie d'une définition. Face à ce silence, la doctrine a tendance à assimiler l'information concernant une personne physique identifiée à l'information concernant une personne physique directement identifiante[421]. Toutefois, puisque la définition légale emploie la conjonction de coordination « ou », une différence se doit d'être opérée.

Selon le groupe des autorités de protection des données (G29), « on peut considérer une personne physique comme "identifiée" lorsque, au sein d'un groupe de personnes, elle se "distingue" de tous les autres membres de ce groupe. La personne physique est donc "identifiable" lorsque, même sans avoir encore été identifiée, il est possible de le faire (comme l'exprime le suffixe "-able") »[422]. Le critère qui ressort de la distinction proposée par le G29 est lié au pouvoir d'user d'une possibilité. Toutefois, un tel critère est très abstrait, d'autant qu'en pratique, c'est surtout le traitement pouvant être effectué sur la donnée qui détermine si celle-ci se rapporte ou non à une personne physique[423]. Par exemple, le nom de famille est insuffisant pour distinguer une personne du reste de la population d'un pays, mais il suffit sans doute pour identifier un élève au sein d'une classe.

En pratique, nous considérons que l'information concernant une personne physique identifiée fait plutôt écho à l'action d'identification effectuée lors de l'utilisation d'un service numérique, c'est-à-dire le fait pour l'utilisateur d'un site Internet d'entrer un identifiant et un mot de passe[424]. Les données générées à partir de l'activité de cette personne identifiée doivent être considérées comme des informations

---

[421] Par exemple, Madame Jessica Eynard définit la personne identifiée comme « la personne dont on connaît l'identité », v. J. Eynard, « Une application systématique du RGPD ? », *Juris tourisme* 2018, nº 207, p. 19.
[422] G29, WP136, Avis 4/2007 du groupe de travail relatif au concept de données à caractère personnel, 20 juin 2007, p. 13.
[423] D'ailleurs, c'est le critère retenu par le législateur dans le considérant 26 du règlement européen, lequel prévoit que pour « déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage ».
[424] C'est le cas par exemple de l'identification sur un compte utilisateur de réseau social.

relatives à une « personne identifiée ». En effet, puisque l'utilisateur identifié génère des données directement liées à son profil, ces données se rapportent nécessairement à lui.

Quelle que soit la définition retenue de l'information concernant une personne physique identifiée, cette catégorie doit être interprétée largement puisqu'elle permet d'inclure non seulement la personne ayant été identifiée, mais aussi la personne qui s'est elle-même identifiée.

114. La nature incertaine du rattachement direct. La définition légale de la donnée à caractère personnel laisse à penser que certaines données permettent un rattachement certain, ou au moins direct, avec une personne physique. La réalité est toutefois plus nuancée. En effet, certaines des données directement identifiantes ne suffisent pas à garantir, avec certitude, l'identification d'une personne physique. Par exemple, en cas d'homonymie, deux personnes avec les mêmes noms et prénoms (informations pourtant, en principe, directement identifiantes) peuvent être confondues. Ainsi, Monsieur Christian Y., né le 2 novembre 1953, s'est vu refuser un crédit à la consommation par un grand magasin et relancer par un organisme de crédit l'ayant signalé comme mauvais payeur, pour des faits issus d'activités d'un autre Monsieur Christian Y., également né le 2 novembre 1953[425]. Les cas d'homonymie montrent le caractère incertain de l'identification des informations issues de l'état-civil[426].

Par ailleurs, il n'est pas impossible qu'un tiers s'empare de données directement identifiantes et les utilise en vue de se faire passer pour la personne concernée. Il s'agit de cas d'usurpation d'identité[427]. Même les informations marquées dans la chair d'une personne, telle que l'empreinte digitale, peuvent être usurpées et utilisées à son insu.

---

[425] Cass. crim., 19 déc. 1995, nº 94-81.431, *Bull. crim.* 1995, nº 387, p. 1133.

[426] D'ailleurs, lorsqu'une homonymie est à l'origine de confusions préjudiciables au requérant, elle justifie son intérêt légitime pour une modification de son prénom, v. *JCl. civil code,* art. 60, fasc. unique, « Actes de l'état civil. Changement de prénom », par C. Marie, 2017, nº 135. Le droit pénal sanctionne également les manœuvres frauduleuses pouvant résulter dans des cas d'homonymies, v. *Rép. pén.* Dalloz, *Vº* « Escroquerie », par C. Mascala, 2016 (actu. 2019), nºs 32 s.

[427] L'usurpation d'identité est considérée comme une atteinte à la vie privée. Selon l'article 226-4 du code pénal, l'usurpation d'identité consiste à « 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 ». Une proposition de loi de 2013 la définissait également comme « le fait de prendre, délibérément, l'identité d'une autre personne vivante pour réaliser des actions frauduleuses commerciales, civiles ou pénales, accéder aux finances de la personne usurpée, ou commettre en son nom un délit, ou accéder à des droits (indemnités sociales) de façon indue », v. proposition de loi de Monsieur Marc Le Fur visant à aggraver la sanction pénale applicable à l'usurpation d'identité commise par le biais de réseaux de communication électronique, Assemblée nationale, nº 1316, déposée le 24 juill. 2013.

En effet, il est aujourd'hui possible de reproduire les empreintes digitales d'une personne avec une imprimante en trois dimensions, notamment pour les utiliser dans le but de se faire passer pour elle[428].

Même si ces deux exemples découlent de situations très différentes, puisque dans un cas la confusion est accidentelle alors que dans l'autre elle est orchestrée, ils illustrent l'incertitude quant au rattachement existant entre une donnée et une personne, et cela même lorsque les données sont directement identifiantes ou relatives à une personne identifiée[429]. La volonté d'englober dans la définition de donnée à caractère personnel le plus d'informations possibles se confirme particulièrement avec l'application de la notion aux informations indirectement identifiantes.

B. L'identification indirecte de la personne

115. Les informations relatives à une personne physique identifiable. Dans la notion de donnée à caractère personnel, à côté des informations intrinsèquement identifiantes, se trouvent également les informations relatives à une *personne physique identifiable*. Pour déterminer si une personne physique est identifiable, l'article 4 du règlement européen prévoit que « est réputée identifiable une personne qui peut être identifiée, directement ou indirectement ». L'identification est donc liée au pouvoir identifiant de la donnée, c'est-à-dire à sa capacité de distinguer, de façon unique, une personne parmi d'autres au sein d'un groupe ou d'un ensemble[430].

116. Plan. Les données indirectement identifiantes sont très variées (1) et incluent notamment les données pseudonymisées (2). Pour éviter une application trop automatique de la notion de donnée à caractère personnel, le législateur a proposé un critère pour la cantonner. L'encadrement qui en ressort se révèle inefficace (3).

---

[428] V. par ex. J. Engelsma, S. Arora, A. Jain et N. Paulter, « Universal 3D wearable fingerprint targets : advancing fingerprint reader evaluations », *IEEE Transactions on Information Forensics and Security* 2018, vol. 13, n° 6. Un autre exemple est celui de l'utilisation d'une photographie en lieu et place du visage du détenteur pour activer certains téléphones Samsung, v. M. Untersinger et M. Tual, « Déverrouiller son iPhone avec son visage : les réponses à vos questions », *Le Monde* 13 sept. 2017, et Le Monde, « Le scanner oculaire du Samsung S8 facilement contournable », *Le Monde* 24 mai 2017.

[429] D'ailleurs, « pour identifier le plus sûrement possible une personne, le droit se réfère aujourd'hui aux caractères les plus fiables à cet égard, à ceux qui demeurent stables : les gènes et les éléments physiques », v. J. Rochfeld, *Les grandes notions du droit privé,* 2e éd., PUF, 2013, *Vo* « La personne », n° 21, p. 45.

[430] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vo* « Identité », sens 1. A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, n° 505, p. 222 ; A. Marais, *Droits des personnes*, 3e éd., Dalloz, 2018, n° 123, p. 88.

1. Les nombreuses informations permettant de faire un lien avec une personne

117. Le foisonnement d'exemples proposés par le législateur. Pour illustrer la variété des données se rapportant à une personne physique, le législateur européen a proposé une longue et non exhaustive liste d'exemples. Cette liste comprend des données telles que « un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou [les] éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »[431]. Ainsi, pour qu'une donnée soit qualifiée de donnée à caractère personnel, il suffit qu'elle se rapporte, même éventuellement, à une personne physique[432].

118. Une application systématique. Selon cette approche extensive, toute donnée semble pouvoir entrer dans la notion de donnée indirectement identifiante, même lorsque la donnée doit être complétée par beaucoup d'autres informations identifiantes ou qu'elle n'est liée à une personne que de manière très éloignée. Ce sont bien les informations qui participent au processus d'identification, même si cette identification n'est qu'éventuelle ou particulièrement compliquée, qui sont couvertes par la définition de donnée à caractère personnel. Ainsi, le lien, même incertain ou distendu, entre une information et une personne physique déclenche la qualification de donnée à caractère personnel. Cette approche est particulièrement significative puisque la notion de donnée à caractère personnel accueille également les données pseudonymisées.

2. Les données pseudonymisées entrant dans la notion de donnée à caractère personnel

119. La notion de désidentification. Il n'existe pas, en droit positif, de définition juridique de l'information désidentifiée. Une directive de 2003 définissait tout de même la désidentification comme « la suppression dans les comptes rendus soumis de tous les détails personnels concernant le notifiant et des aspects techniques qui pourraient permettre d'identifier le notifiant ou des tiers à partir des informations »[433]. Ainsi,

---

[431] Art. 4 § 1 du règlement UE nº 2016/679.
[432] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 493, p. 216.
[433] Art. 2 de la directive CE nº 2003/42 du Parlement européen et du Conseil du 13 juin 2003 concernant les comptes rendus d'événements dans l'aviation civile, *JOCE* 4 juill. 2003, L-167/23, p. 23 s. Cette directive a été abrogée par le règlement UE nº 376/2014 du Parlement européen et du Conseil du 3 avr. 2014 concernant les comptes rendus, l'analyse et le suivi d'événements dans l'aviation civile, *JOUE* 24 avr. 2014, L-122/18, p. 18 s.

l'objectif principal de cette technique est d'effectuer un traitement sur des données pour retirer l'élément ou les éléments les rattachant à une personne physique. Pour autant, la suppression d'informations n'efface pas toujours le lien entre la donnée à la personne[434], c'est pourquoi il existe en réalité deux techniques de désidentification[435]. D'une part la pseudonymisation, et d'autre part l'anonymisation[436]. La distinction entre ces techniques est importante puisque, dans le premier cas, les données entrent dans la notion de données à caractère personnel, alors que dans le second cas, elles en sont exclues[437].

120. La pseudonymisation. La pseudonymisation est une « technique qui consiste à remplacer un identifiant (ou plus généralement des données à caractère personnel) par un pseudonyme »[438]. Pour le règlement européen, la pseudonymisation est une technique effectuée sur des données afin que « celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »[439]. La pseudonymisation suppose donc la réunion de trois conditions :

(1) d'abord le remplacement d'un identifiant par un pseudonyme,

(2) ensuite une conservation séparée des clés de réidentification,

---

Ce texte définit les informations désidentifiées comme « les informations provenant des comptes rendus d'événements dans lesquels toutes les données à caractère personnel, telles que les noms ou adresses des personnes physiques, ont été effacées », v. art. 2 § 6 du règlement UE nº 376/2014.

[434] Par exemple, en 1996, le Gouverneur Weld avait assuré, lors de la mise à disposition publique d'une base de données de santé présentée comme anonymisée, l'impossibilité de réidentifier les individus. Pourtant, Madame Latanya Sweeney avait réussi, grâce aux informations contenues dans les listes électorales, à réidentifier le Gouverneur Weld. Elle avait ainsi démontré que le seul retrait d'informations d'une base de données ne permet pas d'empêcher toute réidentification, v. L. Sweeney, « Weaving Technology and policy together to maintain confidentiality », *The Journal of Law, Medicine and Ethics* 1997, vol. 25, p. 98 s. [25 J.L. MED. & ETHICS 98], spéc. p. 102.

[435] F. Lesaulnier, « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz IP/IT* 2016, p. 573 ; O. Tambou, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, nº 68, p. 60 s.

[436] Sur ces notions, v. S. Stalla-Bourdillon et A. Knoight, « Anonymous data v. personal data. A false debate : an EU perspective on anonymization, pseudonymization and personal data », *Wisconsin International Law Journal* 2017, vol. 34, p. 284 s. [34 WISC. INT'L L.J. 284]. Le G29 distingue les techniques d'anonymisation de celles liées à la pseudonymisation, G29, WP 216, Avis 5/2014 sur les techniques d'anonymisation, 10 avr. 2014, p. 3.

[437] Ces différences seront étudiées plus en détail, v. *infra*, nº 119.

[438] CNIL, « Pack de conformité Logement social », juill. 2014, p. 51. Pour une analyse des techniques de pseudonymisation, v. R. Hu, S. Stalla-Bourdillon, M. Yang, V. Schiavo et V. Sassone, « Bridging policy, regulation and practice ? A techno-legal analysis of three types of data in the GDPR », in *Data protection and privacy. The age of intelligent machines*, dir. R. Leenes, R. van Brakel, S. Gutwirth et P. De Hert, Bloomsbury Publishing, 2017, p. 126 s.

[439] Art. 4 § 5 du règlement UE nº 2016/679.

(3) et enfin des mesures techniques et organisationnelles tendant à empêcher la réidentification[440].

Cette technique ne doit pas être confondue avec le pseudonyme, lequel renvoie à « un nom de fantaisie librement choisi par une personne pour masquer au public sa personnalité véritable dans l'exercice d'une activité particulière »[441]. Toutefois, dans les deux cas, la personne reste réidentifiable et les données entrent donc dans la notion de donnée à caractère personnel, en tant qu'identifiant indirect.

121. Les effets des techniques de pseudonymisation. La pseudonymisation n'empêche pas une réidentification postérieure des personnes concernées puisqu'elle est réversible. Il s'agit plutôt d'un moyen de traiter des données de manière plus protectrice[442], permettant d'effectuer des corrélations, tout en évitant le traitement de données directement identifiantes. À ce titre, la pseudonymisation est présentée, tout au long du règlement européen, comme une garantie à la protection des données à caractère personnel[443]. Celle-ci réduit les risques liés aux traitements : comme moins de personnes ont accès aux informations directement identifiantes, moins d'abus risquent de se produire[444]. En pratique, certains services génèrent des identifiants aléatoires pour éviter de créer une correspondance entre la personne et la donnée générée, ce qui rend la réidentification encore plus complexe[445]. Ainsi, il est possible que le fournisseur du service n'ait pas la correspondance entre la donnée pseudonymisée et la personne.

---

[440] Art. 4 § 5 du règlement UE nº 2016/679.

[441] Cass. civ. 1re, 23 févr. 1965, nº 62-13.427, *Bull. civ.* 1965, nº 148. V. déjà, R. Savatier, obs. ss CA Paris, 23 mai 1924, *DP* 1925, p. 9. En littérature, l'une des premières traces de l'usage moderne de ce terme se trouve dans *Eugénie Grandet* où Balzac fait prendre à Charles Grandet le *pseudonyme* de Chippart « pour ne pas compromettre son nom ».

[442] A. Debet, « Les nouveaux instruments de conformité », *Dalloz IP/IT* 2016, p. 592.

[443] La pseudonymisation est « mentionnée au titre des garanties appropriées qui constituent l'un des critères permettant de déterminer le caractère compatible de la finalité secondaire d'un traitement avec sa finalité initiale (art. 6 § 4) ; c'est également une garantie inhérente au traitement de 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, et un moyen concret d'assurer le respect du principe de minimisation des données dès lors qu'elle est compatible avec la finalité du traitement (art. 89). C'est aussi une mesure concourant à la minimisation des données dès la conception (art. 25), une des mesures appropriées à mettre en œuvre par le responsable du traitement et le sous-traitant pour garantir un niveau de sécurité adapté au risque (art. 32) et pouvant faire l'objet de codes de conduite (art. 40) », F. Lesaulnier, « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz IP/IT* 2016, p. 573. Pour une critique de la pseudonymisation comme « garantie appropriée », particulièrement en matière de données sensibles, v. C. Koumpli, *Les données personnelles sensibles. Contribution à l'évolution du droit fondamental à la protection des données à caractère personnel*, th. Paris I, 2019, p. 442 s.

[444] V. not. cons. 68 du règlement UE nº 2016/679. V. aussi G29, WP 216, Avis 5/2014 sur les techniques d'anonymisation, 10 avr. 2014, p. 3.

[445] Par exemple, la fonctionnalité Siri développée par Apple a recours à ce type de méthode, v. Apple, « Ask Siri, dictation & privacy », 28 oct. 2019.

Par ailleurs, en cas de violation de données, c'est-à-dire en cas de perte ou d'accès non autorisé aux données, les dangers liés à l'identification des personnes sont réduits. La pseudonymisation est donc une technique utilisée pour publier des informations qui ne contiennent pas ou ne contiennent plus de données à caractère personnel directement identifiantes. Par exemple, la jurisprudence française est publiée sur Internet sans les noms des parties et des témoins afin d'éviter leur identification immédiate[446].

122. L'application du droit des données personnelles aux données pseudonymisées. Puisque les données pseudonymisées permettent une réidentification des personnes physiques, elles restent considérées comme des données à caractère personnel, et les principes de ce droit continuent de leur être applicables[447]. Bien qu'une telle qualification soit cohérente parce que ces données sont des données indirectement identifiantes, elle est surtout le témoin d'une conception large de l'identification indirecte, laquelle ne trouve pas vraiment de limite.

3. L'illusoire cantonnement de la notion de donnée à caractère personnel

123. Les limites apparentes à la notion de donnée à caractère personnel. Depuis 1995, le législateur européen propose de border la notion de donnée à caractère personnel en faisant référence aux moyens « raisonnablement susceptibles d'être mis en œuvre » pour identifier une personne[448]. Le considérant 26 du règlement européen prévoit ainsi que pour « déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens *raisonnablement*

---

[446] V. *infra*, nº 265.

[447] Cette interprétation a été débattue à l'occasion des négociations du projet de règlement européen : certains *lobbys* souhaitaient ainsi que les données pseudonymisées ne soient pas considérées comme des données personnelles, v. F. Lesaulnier, « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz IP/IT* 2016, p. 573.

[448] Lors de la transposition de la directive CE nº 95/46, le législateur français avait refusé d'introduire l'adverbe « raisonnablement » qui figurait pourtant dans ce texte. Selon Monsieur Francis Delattre, rapporteur à l'Assemblée nationale, « l'emploi de l'adverbe "raisonnablement" n'est pas sans ambiguïté et risque de provoquer de réelles difficultés d'interprétation, sources de contentieux », F. Delattre, « Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », Assemblée nationale, nº 1537, 13 avr. 2004, p. 11 s. À l'inverse, le rapporteur au Sénat, Monsieur Alex Türk, était favorable à une telle introduction en considérant que cet adverbe permettait de « préciser la distinction entre données anonymes et données indirectement nominatives », v. A. Türk, « Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », Sénat, nº 218, 19 mars 2003, p. 48.

susceptibles d'être utilisés par le responsable du traitement ou *par toute autre personne* pour identifier la personne physique directement ou indirectement »[449].

À première vue, l'adverbe « raisonnablement » réduit le champ d'application de la notion puisque, comme l'affirment certains auteurs, il permet d'encadrer cette définition[450]. En réalité, son interprétation est loin d'atteindre un tel résultat. En effet, pour savoir si une donnée est indirectement identifiante, les responsables du traitement doivent déterminer les moyens susceptibles d'être mis en œuvre non seulement au sein de leur organisme, mais surtout par « toute autre personne ». L'analyse du caractère raisonnable des moyens susceptibles d'être utilisés pour réidentifier une personne diverge drastiquement entre les responsables du traitement. Par exemple, les services de renseignement — tels que la National Security Agency (NSA) ou la Direction générale de la Sécurité extérieure (DGSE) — ou les grandes entreprises privées — telles que Criteo, Facebook ou Google — n'ont absolument pas les mêmes capacités de réidentification que des plus petites structures telles que le bureau de police local ou des entreprises comme Carrefour ou OVH. En adoptant un standard abstrait, c'est-à-dire sans lien avec les capacités réelles du responsable du traitement ou de son sous-traitant, le législateur pose un principe de qualification quasi automatique des données en données à caractère personnel[451]. En effet, ce sont les acteurs les plus puissants, lesquels disposent d'un très grand nombre de données et de fortes capacités de traitement de l'information, qui déterminent, *de facto*, le standard pour tous les autres acteurs. La limite posée par le législateur se révèle donc illusoire puisque, dans la plupart des cas, un tiers aux fortes capacités de traitement pourra effectivement réidentifier la personne à partir de la donnée indirectement identifiante.

En tout état de cause, cette subjectivité engendre une insécurité juridique pour les responsables du traitement. En cas de litige, les juges devront déterminer *a posteriori* quels moyens le responsable du traitement ou toute autre personne aurait pu raisonnablement utiliser, au moment des faits, pour identifier une personne physique.

---

[449] Le considérant 26 de la directive CE nº 95/46 prévoyait des dispositions similaires.
[450] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 527, p. 230.
[451] Cela rappelle d'ailleurs l'interprétation large retenue de l'identification, notamment pour la voix. Ainsi, les juges du fond ont considéré que la voix peut bénéficier de la protection instituée par l'article 9 du code civil « dans la mesure où une voix caractéristique peut être rattachée à une personne identifiable », même si cette identification n'est possible que pour une connaissance ou un membre de la famille, v. CA Pau, 22 janv. 2001, nº 99/00051, *D.* 2002, p. 2375.

Le principal risque étant alors la requalification en données à caractère personnel de données n'ayant pas été considérées comme telles[452].

En définitive, ce critère de cantonnement n'est qu'une façade et encourage également une conception large de la notion. Seules les données pour lesquelles ce rattachement est impossible ou inexistant, ne sont pas qualifiées comme des données à caractère personnel.

C. L'identification impossible de la personne

124. Les données exclues du champ d'application du règlement européen. Le règlement européen exclut de son champ d'application les informations anonymes[453]. Selon ce texte, les informations anonymes sont de deux types : soit elles ont été, par le passé, en lien avec une personne physique[454] ; soit elles n'ont jamais eu ce lien. Dans ce dernier cas, le qualificatif « d'information anonyme » surprend. En effet, en droit, l'adjectif « anonyme » renvoie à l'impossibilité de faire un lien avec une personne, voire à l'absence de nom, mais ne renvoie pas à l'absence absolue de lien avec une personne[455]. Par exemple, pour une œuvre anonyme, c'est-à-dire l'œuvre d'un auteur inconnu[456], il est évident qu'une personne a créé cette œuvre. Toutefois, le lien entre l'auteur et l'œuvre ne peut pas être effectué[457]. Autre exemple, pour le don de gamètes, il est évident qu'elles proviennent bien d'une personne physique mais les règles bioéthiques imposent l'anonymat entre le donneur et le receveur[458]. Ainsi, l'utilisation de ce terme pour des données n'ayant jamais eu de lien avec la personne génère une confusion certaine.

Lorsque les données n'ont jamais eu de lien avec les personnes, comme c'est le cas par exemple pour les ingrédients composants un produit ou les données liées à la météo, une simple référence à la notion de « donnée » aurait suffi. Le fait que le législateur préfère avoir recours à la notion de données anonymes pour ces données est

---

[452] V. not. les faits de la décision Cass. civ. 1re, 3 nov. 2016, nº 15-22.595, *Bull. civ.* 2016, nº 206, p. 251.
[453] Pour une analyse des interactions entre anonymat et droit, v. J.-C. Saint-Pau, *L'anonymat et le droit*, th. Bordeaux, 1998 ; J. Pousson-Petit, « Le droit à l'anonymat », in *Mélanges L. Boyer*, PU Toulouse, 1996, p. 596 s.
[454] Elles ont ensuite été traitées « de telle manière que la personne concernée ne soit pas ou plus identifiable », v. cons. 26 du règlement UE nº 2016/679.
[455] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vº* « Anonyme », sens 1 et 2.
[456] M. Vivant et J.-M. Bruguière, *Droit d'auteur et droits voisins*, 4e éd., Dalloz, 2019, nº 116, p. 167 s.
[457] P.-Y. Gautier, *Propriété littéraire et artistique*, 11e éd., PUF, 2019, nº 212, p. 242 ; *JCl. civil annexes, Vº* Propriété littéraire et artistique, fasc. 1134, « Objet du droit d'auteur. Œuvres protégées. Notion d'œuvre », par A. Bensamoun et J. Goffre, 2019, nº 11.
[458] C. Labrusse-Riou, « L'anonymat du donneur : étude critique de droit positif français », in *Écrits de bioéthique,* dir. C. Labrusse-Riou et M. Fabre-Magnan, PUF, 2007, p. 196.

une illustration de sa volonté de voir appliquer la notion de donnée à caractère personnel très largement. L'étude des notions de données anonymisées et des données non personnelles confirme cette impression.

125. Les données anonymisées. En droit des données personnelles, la technique d'anonymisation consiste à retirer suffisamment d'éléments dans des données pour que la personne concernée ne puisse plus être identifiée[459]. Plus précisément, il s'agit de modifier le contenu ou la structure des données « en utilisant tous les moyens pouvant être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne » afin de ne plus pouvoir identifier une personne physique[460]. L'un des éléments essentiels de l'anonymisation est que le traitement est *irréversible*, c'est-à-dire qu'aucun traitement futur ne doit permettre de réidentifier les personnes physiques[461]. Ainsi, pour le Conseil d'État, une donnée « ne peut être regardée comme rendue anonyme que lorsque l'identification de la personne concernée, directement ou indirectement, devient impossible, que ce soit par le responsable du traitement ou par un tiers. Tel n'est pas le cas lorsqu'il demeure possible d'individualiser une personne ou de relier entre elles des données résultant de deux enregistrements qui la concernent »[462]. Une fois rendues anonymes, les données ne sont plus considérées comme des données à caractère personnel[463], c'est-à-dire qu'elles ne sont plus soumises aux principes de protection et peuvent donc être utilisées librement[464].

126. La présomption du caractère personnel des données. En principe, en vertu du principe de libre circulation de l'information[465], la simple donnée a un champ d'application plus étendu que celui de la donnée à caractère personnel. Il suffit de

---

[459] Cons. 26 du règlement UE nº 2016/679 et G29, WP 216, Avis 5/2014 sur les techniques d'anonymisation, 10 avr. 2014, p. 6.
[460] Le considérant 26 de la directive CE nº 95/46 donnait une définition conceptuelle de l'anonymisation qui a été reprise par le G29 dans son avis sur les techniques d'anonymisation, G29, WP 216, Avis 5/2014 sur les techniques d'anonymisation, 10 avr. 2014, p. 6.
[461] G29, WP 216, Avis 5/2014 sur les techniques d'anonymisation, 10 avr. 2014, p. 7.
[462] CE Sec., 8 févr. 2017, *JC Decaux France*, nº 393714, *Lebon T*. p. 614, § 7. Pour une analyse de cette décision, v. N. Métallinos, « Anonymisation et pseudonymisation. Le Conseil d'État enterre l'analyse des flux piétons *via* WIFI », *CCE* 2017, nº 4, comm. 37.
[463] Le traitement effectué sur des données dans le but d'anonymiser ces données reste quant à lui considéré comme un traitement de données à caractère personnel, G29, WP 216, Avis 5/2014 sur les techniques d'anonymisation, 10 avr. 2014, p. 7.
[464] O. Tambou, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, nº 68, p. 61.
[465] V. *supra,* nº 77.

consulter les sites accueillant des bases de données ouvertes pour s'en convaincre[466]. Par exemple, la base de données communautaire « Open Food Facts » qui recense les données sur les produits alimentaires telles que les ingrédients, les informations nutritionnelles ou les labels, renseigne sur les produits alimentaires sans qu'un lien entre ces données et une personne physique ne soit possible[467]. Il en va de même pour les bases de données comptables et fiscales d'un établissement public ou d'une collectivité locale informant sur les dépenses et les recettes de ces établissements. Il en va également ainsi pour les quelques 2,5 téraoctets de données générées quotidiennement par un avion[468]. Pourtant, le prisme de la protection des personnes tend à effacer cette réalité et les textes adoptés récemment s'inscrivent dans un mouvement de personnalisation des données. Par exemple, le règlement européen relatif au libre flux des données à caractère non personnel a défini les simples données comme « les données autres que les données à caractère personnel »[469]. En consacrant la définition de données par opposition aux données à caractère personnel, le législateur européen renverse le point de départ de la qualification[470]. Selon cette conception, les données sont, par principe, en lien avec une personne physique.

Le renversement du point de départ de la qualification n'est pas neutre pour la conception générale de la notion de donnée. Il induit *a priori* un lien potentiel avec une personne physique. En réalité, l'étude des composantes de la notion montre que celle-ci s'applique par défaut et que, dans certains cas, il est parfois possible de réfuter cette qualification.

127. Conclusion de chapitre. Pour qu'une donnée soit qualifiée de donnée à caractère personnel, trois éléments doivent être réunis : une donnée, une personne physique et le rattachement des deux. L'étude de chacun de ces éléments montre que cette notion a été élaborée pour couvrir toutes les hypothèses où une donnée peut se

---

[466] Sur le mouvement des données ouvertes, v. not. le dossier « Les enjeux de l'open data », *AJDA* 2016, n° 2, p. 79 s. V. aussi, *Rép. cont. adm.* Dalloz, *V°* « Communication des documents administratifs », par A. Lallet et P. Nguyen Duy, 2019, n^os^ 2 s.

[467] La base de données Open Food Facts est une base de données libre relative aux produits alimentaires. Elle est utilisée par d'autres applications pour informer les personnes, notamment par l'application Yuka qui décrypte les étiquettes des produits alimentaires et cosmétiques et analyse leur impact sur la santé des personnes.

[468] Airbus, « Data revolution in aviation ». Airbus a annoncé que son nouvel avion, le A350, avait quelques 50 000 capteurs à bord collectant quotidiennement 2,5 téraoctets de données.

[469] Art. 3 § 1 du règlement UE n° 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, *JOUE* 28 nov. 2018, L-303/65, p. 65 s.

[470] D'ailleurs, comme le remarquait Madame Célia Zolynski, ce choix est effectué volontairement par le législateur européen puisque la « priorité est donnée au RGPD », v. C. Zolynski, « La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne », *Dalloz IP/IT* 2020, p. 429.

rapporter, même très indirectement, à une personne physique. Cela ressort d'abord dans le choix du terme « donnée », préféré à celui moins élastique d'information ou de document. Ce ressort ensuite de la notion de personne physique au sens du droit des données à caractère personnel, laquelle ne se cantonne pas aux contours dessinés traditionnellement par le droit civil. Les données relatives à des enfants à naître ou à des personnes décédées y trouvent parfois une place. D'autres fois, ce sont les personnes morales qui entrent dans celle-ci. Enfin, le lien entre la personne et la donnée peut s'avérer très souple, dès lors qu'il inclut non seulement les cas dans lesquels le rattachement est direct, mais aussi les cas dans lesquels l'identification n'est que potentielle, voire incertaine. Dans ces derniers cas, les frontières de l'identification s'élargissent au rythme des technologies et la notion accueille de plus en plus de données. Les mécanismes juridiques prévus pour cantonner cette notion, tels que l'encadrement par les moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou les tiers, ne parviennent pas à contenir cet élargissement. L'ensemble de ces éléments encourage l'essor de la notion.

Chapitre II – L'essor de la notion de donnée à caractère personnel

128. Un mouvement continu. Comme le remarquait Portalis, les hommes « ne se reposent jamais ; ils agissent toujours : et ce mouvement, qui ne s'arrête pas, et dont les effets sont diversement modifiés par les circonstances, produit, à chaque instant, quelque combinaison nouvelle, quelque nouveau fait, quelque résultat nouveau »[471]. L'homme n'est pas le seul à être en mouvement : la science, les mœurs, l'économie se transforment et invitent encore et toujours le droit à s'adapter[472]. En matière de données à caractère personnel, ce mouvement est particulièrement notable parce qu'il dépend de la célérité avec laquelle les technologies se développent. Pour répondre aux attentes de la société et garantir aux personnes une protection cohérente de leurs informations, la notion de donnée à caractère personnel doit donc continuellement s'ajuster.

129. L'évolution de la notion. Adoptée à la fin des années 1970, la notion de donnée personnelle a connu un essor remarquable. Mal connue du juriste de la seconde moitié du XX^e^ siècle, elle se retrouve aujourd'hui dans tous les domaines du droit. Le développement fulgurant des technologies de collecte de données, ainsi que la densification de l'utilisation des données ont accéléré la mutation de cette notion. Celle-ci s'est effectuée à la faveur d'une acception large.

130. Plan. L'étude des manifestations de l'essor de la notion (Section I) précèdera celle de ses causes (Section II).

SECTION I – LES MANIFESTATIONS DE L'ESSOR DE LA NOTION

131. Plan. Plusieurs acteurs de la protection des données à caractère personnel ont contribué à l'essor de la notion. Le législateur d'abord, qui a choisi une terminologie très large permettant de couvrir l'ensemble des situations dans lesquelles une donnée peut être liée à une personne (§ I). Cette terminologie est interprétée de manière accueillante par les autorités de protection et les juges afin de faire entrer dans la notion

[471] J.-É.-M. Portalis, *Discours préliminaire au premier projet de Code civil*, Confluences, 1999, p. 17.
[472] J.-L. Bergel, *Théorie générale du droit*, 5^e^ éd., Dalloz, 2012, n^o^ 102, p. 128 s.

toutes les informations qui peuvent avoir un rapport avec une personne, même lorsque ce rapport est incertain ou indirect (§ II).

§ I. Le rôle du législateur dans l'expansion

132. Plan. Animé par la volonté de protéger les données relatives aux personnes quel que soit le secteur d'activité, les législateurs français et européen ont adopté une législation d'ensemble. Ce choix a des conséquences sur la notion puisque celle-ci doit être suffisamment large et flexible pour s'adapter aux spécificités de chacun des secteurs d'activité (A). Le glissement sémantique de la notion d'information nominative à celle de donnée à caractère personnel témoigne du besoin d'adaptabilité de la notion (B). Enfin, la coexistence des « simples données » et des données sensibles a également contribué à l'appréhension large de la notion de donnée à caractère personnel (C).

A. Une législation d'ensemble propice à l'élargissement notionnel

133. Deux modèles de protection des données. Comme l'expliquait Guy Braibant, « deux solutions s'offrent aux législateurs lorsqu'ils doivent règlementer les problèmes nouveaux nés du développement de l'informatique : donner lieu à un texte d'ensemble ou à une série de textes particuliers relatifs à chacun des secteurs intéressés, tels que la médecine ou les statistiques »[473]. Cette dualité d'approche se retrouve dans les deux tendances mondiales de protection des données à caractère personnel. D'un côté, le modèle issu du droit de l'Union européenne, fondé sur un ensemble transversal de règles applicables à tous les secteurs d'activité[474], et de l'autre, le modèle des États-Unis d'Amérique, fondé sur une multitude de règles étatiques et fédérales règlementant

[473] G. Braibant, « La protection des droits individuels au regard du développement de l'informatique », *RID comp.* 1971, vol. 23, nº 4, p. 793, spéc. p. 801.

[474] Le modèle européen est souvent présenté comme un modèle *omnibus*, v. C. Castets-Renard, « Quels liens établir entre les USA et l'UE en matière de vie privée et protection des données personnelles ? », *Dalloz IP/IT* 2016, p. 115. Pour autant, déjà en 1998, Guy Braibant avait identifié une trentaine de lois relatives aux données à caractère personnel, atténuant ainsi la pertinence de cette expression pour qualifier le droit français, v. G. Braibant, « Données personnelles et société de l'information. Rapport au Premier ministre sur la transposition en droit français de la directive nº 95/46 », La Documentation française, 1998, p. 18. Aujourd'hui encore, plusieurs règles spéciales coexistent à côté du règlement UE nº 2016/679, notamment la directive UE nº 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, *JOUE* 4 mai 2016, L-119/89, p. 89 s. ; ainsi que la règlementation en matière de communications électroniques (notamment le « paquet Télécom »), v. *Rép. eur.* Dalloz, *Vº* « Télécommunications et communications électroniques », par L. Rapp, 2005 (actu. 2019), nºs 112 s.

les traitements de données selon les secteurs d'activité[475]. Les pays tiers s'inspirent souvent de ces modèles pour réglementer leurs traitements de données personnelles[476].

134. Le modèle sectoriel et la variété notionnelle. Aux États-Unis d'Amérique, la protection des données d'une personne navigue entre différents domaines juridiques. Elle est composée de règles issues du droit constitutionnel étatique et fédéral, de la responsabilité civile, de règles de procédure, du droit des biens, du droit des contrats, du droit de la concurrence, du droit pénal et de lois étatiques et fédérales sectorielles[477]. En 1973, le rapport sur les « Renseignements, les ordinateurs et les droits des citoyens »[478] avait posé la première pierre à l'édification d'une législation américaine sur la *information privacy*, c'est-à-dire sur la protection des données personnelles[479]. Ce rapport recommandait la création d'un *code of fair information practices*, lequel instituait des principes applicables aux organisations collectant des données personnelles[480]. Ces données alors étaient définies comme les « fichiers contenant des

---

[475] P. Schwartz et D. Solove, *Information privacy law*, 6e éd., Wolters Kluwer, 2018, p. 876.

[476] Le modèle européen est une grande source d'inspiration pour les États tiers. En effet, plusieurs pays tels que le Brésil, le Chili et des pays d'Asie (Inde, Indonésie, Thaïlande, Japon et Corée) se sont largement inspirés de la règlementation européenne à l'occasion de l'élaboration de leurs propres lois, D. Tramacere, « Only good coming out of the new EU data protection regulation », *European Union External Action* 19 sept. 2018. Selon Madame Olivia Tambou, le standard européen est assurément une source d'inspiration pour les États et les organisations internationales, O. Tambou, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, nos 53 s., p. 43 s. À ce titre, il est intéressant de constater que le Contrôleur européen sur la protection des données, dans sa réaction à la décision de la CJUE du 16 juillet 2020, a encouragé les États-Unis à « mettre en œuvre tous les efforts et moyens possibles pour s'orienter vers un système transversal de protection des données à caractère personnel ». Pour autant, rien dans la décision de la Cour n'évoquait un tel besoin, v. EDPS, « Statement following the Court of Justice ruling in Case C-311/18 Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems ("Schrems II") », 17 juill. 2020.

[477] « Information privacy law is an interrelated web of tort law, federal and state constitutional law, federal and state statutory law, evidentiary privileges, property law, contract law, and criminal law », v. P. Schwartz et D. Solove, *Information privacy law*, 6e éd., Wolters Kluwer, 2018, p. 2.

[478] United States Department of Health, Education and Welfare, « Records, computers, and the rights of citizens », 1973.

[479] Plusieurs auteurs utilisent les notions de « *information privacy* » et de « *data protection law* » comme des synonymes, v. M. Burdon, *Digital data collection and information privacy law*, Cambridge University Press, 2000, p. 2. Dans le rapport de 1973, les notions de « *identifiable information* » et de « *personal data* » étaient aussi utilisées comme des synonymes. Pour les besoins de notre démonstration, nous aurons recours au terme générique de donnée personnelle.

[480] United States Department of Health, Education and Welfare, « Records, computers, and the rights of citizens », 1973, p. 41. Ce rapport prévoit une série de principes : « There must be no personal data record-keeping systems whose very existence is secret. There must be a way for a person to find out what information about the person is in a record and how it is used. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent. There must be a way for a person to correct or amend a record of identifiable information about the person. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data », pouvant être traduit par « Il ne doit pas exister de base de données personnelles dont l'existence serait secrète. La personne doit avoir un moyen de savoir quelles informations sont présentes dans la base de données et comment elles sont utilisées. La personne doit pouvoir empêcher que des données collectées pour un objectif soient utilisées ou mises à disposition pour d'autres objectifs sans son consentement. Il doit être prévu une façon pour la personne de rectifier, de modifier un document contenant des informations identifiantes à propos d'elle. Toute organisation créant, maintenant, utilisant ou disséminant des bases de données doit s'assurer de la fiabilité des données et doit s'assurer de prévenir les mauvais usages des données. »

informations identifiantes relatives à un individu »[481]. Cette définition restrictive, mais générique, n'a pas été reprise par les lois sectorielles adoptées postérieurement.

La kyrielle de lois fédérales protégeant les données a son propre champ d'application, et il n'existe donc pas, aux États-Unis, de définition uniforme de ce que recouvre la notion de donnée personnelle. Au contraire, ce sont des définitions multiples, incohérentes et souvent restrictives qui sont prévues par ces textes[482]. Par exemple, la loi relative aux données des enfants de moins de treize ans (COPPA) définit les données personnelles comme « les informations relatives à une personne physique identifiable individuellement »[483] ; la loi relative aux informations liées aux locations de vidéos (VPAA) protège « les informations qui identifient une personne qui a demandé ou obtenu certaines vidéos ou services de la part d'un fournisseur de services vidéo »[484] ; quant à la loi relative à la télévision par câble (*Cable Communications Policy Act*), elle définit les informations personnelles comme « les informations qui ne contiennent pas des données agrégées »[485]. Certaines lois sectorielles établissent même une liste arrêtée de données protégées[486].

135. Une application limitée de la notion par le modèle sectoriel. Ces différentes définitions de la donnée personnelle empêchent l'émergence d'une notion unifiée et cohérente. À cela s'ajoutent également les limites intrinsèques au caractère sectoriel des règles. Elles définissent un périmètre relativement restreint protégeant certaines données, excluant parfois des pans entiers d'informations ayant pourtant un lien avec une personne physique[487]. En effet, les lois ne protègent ces données que lorsqu'elles sont traitées par certains organismes clairement identifiés. Enfin, la plupart de ces lois ont été adoptées à la fin du XX^{e} siècle et visent souvent les données relatives à une

---

[481] United States Department of Health, Education and Welfare, « Records, computers, and the rights of citizens », 1973, p. 41.
[482] P. Schwartz et D. Solove, « Reconciling personal information in the United States and European Union », *California Law Review* 2014, vol. 102, p. 877 s. [102 CALIF. L. REV. 877], spéc. p. 887.
[483] Pub. L. du 21 avr. 2000, n^{o} 105-277, codifiée au 15 U.S.C. § 6501 s. Le *Children's Online Privacy Protection Act* (COPPA) apporte des protections dans le cadre de la collecte en ligne d'informations personnelles d'enfants âgés de moins de 13 ans. La définition des informations personnelles est fournie par l'article 15. U.S.C. § 6501 (8). Pour plus de détails sur les obligations de cette loi, v. *infra*, n^{o} 368.
[484] *Video Privacy Protection Act* de 1988, (VPPA), Pub. L. du 5 nov. 1988, n^{o} 100-618, codifiée au 18 U.S.C. § 2710. La définition des informations personnelles est fournie dans l'article 18 U.S.C. § 2710 (a)(3).
[485] *Cable Communications Policy Act* de 1984, (*Cable Act*), Pub. L. du 30 oct. 1984, n^{o} 98-549, codifiée au 47 U.S.C. § 551. La définition des informations personnelles est prévue par l'article 47 U.S.C. § 551 (a)(2)(A).
[486] P. Schwartz et D. Solove, « Reconciling personal information in the United States and European Union », *California Law Review* 2014, vol. 102, p. 877 s. [102 CALIF. L. REV. 877], spéc. p. 890.
[487] C'est particulièrement le cas lorsque la loi énumère les informations considérées comme données personnelles, notamment pour les lois relatives aux violations de données, v. P. Schwartz et D. Solove, « Reconciling personal information in the United States and European Union », *California Law Review* 2014, vol. 102, p. 877 s. [102 CALIF. L. REV. 877], spéc. p. 889.

personne *identifiée*, excluant toute forme de protection pour les données indirectement identifiantes[488]. Ces règles sectorielles s'opposent à une interprétation transversale et ouverte de la notion de donnée personnelle et favorise, au contraire, une interprétation restrictive.

136. Une application large par le modèle d'ensemble européen. À l'opposé du modèle sectoriel américain se trouve le modèle d'ensemble européen. En appréhendant le droit des données à caractère personnel avec une loi transversale[489], le législateur européen a opté pour une notion générique applicable à tous les secteurs d'activité, favorisant ainsi l'émergence d'une notion flexible. Selon cette approche, la notion doit être suffisamment souple pour envelopper toutes les situations dans lesquels une donnée peut être liée à une personne physique[490]. Cette flexibilité favorise une acception large de la notion de donnée à caractère personnel et encourage son essor.

B. Un glissement sémantique de l'information nominative à la donnée à caractère personnel

137. La notion d'information nominative. En 1978, le législateur français avait retenu la notion d'information nominative pour circonscrire le domaine de la loi Informatique et libertés. Les dictionnaires définissent le terme nominatif comme « ce qui nomme ; qui contient, énonce expressément le nom »[491]. Pour être considérée comme nominative, l'information doit donc se rapporter au nom de la personne qu'elle désigne. Dans les autres domaines juridiques dans lesquels le terme nominatif est utilisé, il indique toujours un lien entre le nom et la personne. Par exemple, en procédure pénale, le « compte nominatif » du détenu désigne le compte *au nom* de la personne détenue[492], et en droit des sociétés, les « actions nominatives » font référence aux actions *au nom* de leur titulaire[493]. Employée avec cette conception du rapport au nom, l'information nominative était de nature à réduire considérablement la portée de

---

[488] P. Schwartz et D. Solove, « Reconciling personal information in the United States and European Union », *California Law Review* 2014, vol. 102, p. 877 s. [102 CALIF. L. REV. 877], spéc. p. 891.
[489] V. *supra*, n° 136.
[490] Ces cas sont très variés car les données collectées par un service bancaire sont très différentes de celles traitées par un réseau social ou celles amassées par un moteur de recherche.
[491] A. Rey et J. Rey-Debove, *Le petit Robert de la langue française*, 2017, Le Robert, *V°* « Nominatif, ive ».
[492] Le compte nominatif est le compte bancaire sur lequel est placé l'argent de la personne détenue dans une prison, v. *Rép. pén.* Dalloz, *V°* « Prison. Organisation générale. Régime de la détention », par J.-P. Céré, 2015 (actu. 2019), n^os^ 200 s.
[493] Les actions nominatives sont les actions dont l'inscription est faite sur les registres de la société émettrice au nom du titulaire de l'action, *Rép. soc.* Dalloz, *V°* « Action. Forme des actions », par J.-F. Artz, 2002 (actu. 2019), n^os^ 89 s.

la loi du 6 janvier 1978[494]. En se fondant sur le qualificatif *nominatif*, la loi écartait de son champ d'application toutes les informations ne permettant pas, en soi, de nommer une personne[495]. En effet, l'adjectif nominatif ne fait pas référence à la capacité objective, abstraite, de l'information à se rapporter à une personne physique, mais fait plutôt référence à la capacité de dénommer, de contenir un nom.

138. La définition légale de l'information nominative. La définition fournie par la loi du 6 janvier 1978 était en total décalage avec les termes de la notion[496]. En effet, les informations nominatives étaient définies par l'article 4 de cette loi comme « les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent. » Cette définition légale, loin de se cantonner aux seules informations relatives au nom, encourageait une interprétation large de la notion et soumettait une grande variété d'informations à la loi. Face à une telle dissonance entre les termes de la notion et sa définition, toute tentative de détermination du domaine de l'information nominative était nécessairement épineuse.

139. L'adoption de la notion de donnée à caractère personnel. La transposition de la directive 95/46[497] a scellé le passage, en droit français, de la notion d'information nominative à celle de donnée à caractère personnel[498]. Ces termes ont été choisis parce qu'ils présentent des caractères de généralité et de neutralité évitant l'obsolescence rapide de la loi[499], et permettent son application à toutes formes de données[500].

---

[494] A. Lucas, J. Devèze et J. Frayssinet, *Droit de l'informatique et de l'Internet*, PUF, 2001, n° 111, spéc. p. 77.
[495] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, n°s 482 s., p. 213 s.
[496] J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 11.
[497] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978, *JORF* du 7 août 2004, n° 0182, p. 14063.
[498] En réalité, le glissement sémantique s'était effectué dès 1980 dans les lignes directrices de l'OCDE, v. OCDE, Lignes directrices du 23 sept. 1980 sur la vie privée et les flux transfrontières de données à caractère personnel. Ce glissement s'était confirmé rapidement, v. Conseil de l'Europe, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* n° 108, 28 janv. 1981 (dite Convention 108).
[499] A. Türk, « Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », Sénat, n° 218, 19 mars 2003, p. 47.
[500] Ainsi, pour la plupart des auteurs, « tous les types d'information-donnée peuvent acquérir le caractère personnel, quels que soient le sens, l'utilité, l'usage, le volume, le support, le mode de représentation », v. A. Lucas, J. Devèze et J. Frayssinet, *Droit de l'informatique et de l'Internet*, PUF, 2001, n° 113, p. 77. V. aussi Commission des communautés européennes, COM (92) 422, « Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data », 15 oct. 1992.

Tout d'abord, la substitution du terme information par le terme générique de donnée favorise une interprétation souple de la notion[501]. Ensuite, l'ajout du terme « caractère » renforce l'aspect indirect de l'identification, puisqu'il fait référence à l'intermédiaire pouvant exister entre la personne et l'identification[502]. Enfin, la substitution du qualificatif « personnel » à celui de « nominatif » efface la référence au nom et renvoie à la notion de personne[503], laquelle inclut de nombreux éléments d'identification.

140. La définition légale de la donnée à caractère personnel. Le législateur européen a retenu, dans la directive de 1995, une définition extrêmement large de la notion de donnée à caractère personnel puisque celle-ci était envisagée comme « toute information concernant une personne physique identifiée ou identifiable »[504]. La loi française de transposition avait repris cette définition à l'identique[505] ; quant au règlement européen[506], il s'en est largement inspiré puisque son article 4 définit la donnée à caractère personnel comme « toute information se rapportant à une personne physique identifiée ou identifiable »[507].

La définition retenue par le règlement européen est encore plus large que celle applicable jusqu'à son adoption. D'une part, la substitution du verbe rapporter au verbe concerner contribue à l'assouplissement du lien entre la donnée et la personne[508]. En effet, le verbe rapporter semble plus souple et favorise l'application de la notion à un plus grand nombre de données. D'autre part, la liste d'identifiants proposée par le règlement européen est beaucoup plus longue que celle qui figurait dans la directive de

---

[501] Sur la distinction entre le terme de donnée et celui d'information, v. *supra*, n° 59.
[502] Le terme « caractère » est emprunté au latin *character*, du grec *kharaktêr*, « signe gravé ; empreinte », puis « signe distinctif propre à une personne », *Dictionnaire de l'Académie française*, 9e éd., *V°* « Caractère », sens II.
[503] Le terme personnel est emprunté au latin *personalis*, c'est-à-dire « relatif à la personne », l'adjectif personnel « se dit de ce qui concerne la personne et non les biens ou les choses », v. *Dictionnaire de l'Académie française*, 9e éd., *V°* « Personnel », sens I.1.
[504] Art. 2 (a) de la directive CE n° 95/46. V. les travaux préparatoires de la Commission des communautés européennes, COM (92) 422, « Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data », 15 oct. 1992, p. 9. Le législateur européen a rejeté la notion plus stricte d'« information nominative ».
[505] Art. 2 de la loi n° 78-17 du 6 janv. 1978 telle que modifiée par la loi n° 2004-801 du 6 août 2004.
[506] Pour une analyse de l'évolution de la définition de la notion de donnée personnelle, v. *JCl. comm.,* fasc. 930, « Données à caractère personnel. Introduction générale et champ d'application de la règlementation relative à la protection des données personnelles », par R. Perray, 2019 (actu. 2020), nos 73 s. ; v. aussi, V.-L. Benabou, « L'extension du domaine de la donnée », *Légicom* 2017, n° 59, p. 3, spéc. p. 4 s.
[507] Selon Monsieur Xavier Tracol, les définitions proposées par le règlement européen sont plus larges que celles retenues dans la directive, X. Tracol, « Le règlement et la directive relatifs à la protection des données à caractère personnel », *Europe* 2016, n° 10, étude 8.
[508] Le verbe rapporter signifie « rattacher une chose à une autre, établir un lien entre plusieurs choses », *Dictionnaire de l'Académie française*, 9e éd., *V°* « Rapporter », sens IV ; alors que le verbe concerner signifie « avoir rapport à », v. É. Littré, *Le nouveau Littré. Le dictionnaire de référence de la langue française*, Garnier, 2007, *V°* « Concerner ».

1995, sans doute pour illustrer la variété d'informations relevant de la notion de donnée à caractère personnel. Le fait que le législateur utilise l'adverbe « notamment » avant d'entamer cette longue liste confirme d'ailleurs cette impression. Ainsi, il ne fait aucun doute que les législateurs français et européen ont adopté une notion très souple et accueillante pour encourager son application à toutes les données pouvant concerner, même très indirectement, une personne[509]. À cette définition déjà large de donnée à caractère personnel s'ajoute également la reconnaissance d'une catégorie particulière de données personnelles.

C. La coexistence entre les simples données à caractère personnel et les données sensibles

141. L'inclusion d'une catégorie particulière de données dans la notion de donnée à caractère personnel. Le concept de donnée à caractère personnel recoupe deux types d'informations[510] : d'une part la *simple donnée à caractère personnel*, c'est-à-dire toutes les informations se rapportant à une personne physique, et d'autre part la *donnée sensible*, c'est-à-dire les informations qui touchent à l'intimité de la personne, celles relatives à ses caractéristiques propres ou celles qui sont susceptibles de donner lieu à des discriminations[511].

142. Les données considérées comme des données sensibles. Déjà en 1978, le législateur français avait consacré un régime particulier pour certaines informations nominatives. Parmi ces données figuraient les informations relatives aux infractions, aux origines raciales, aux opinions politiques, philosophiques, religieuses, à l'appartenance syndicale, au fichier conducteur, électoral, et le numéro d'inscription des personnes au répertoire national d'identification[512]. En 2004, cette notion avait évolué pour mieux prendre en compte les attentes de la société en ce qui concerne la protection des informations les plus intimes. Ainsi étaient qualifiées de données sensibles les données liées aux opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou les données relatives à la santé ou à la vie

[509] V.-L. Benabou, « L'extension du domaine de la donnée », *Légicom* 2017, n° 59, p. 3, spéc. p. 4 s.
[510] Sur cette distinction, v. C. Koumpli, *Les données personnelles sensibles. Contribution à l'évolution du droit fondamental à la protection des données à caractère personnel*, th. Paris I, 2019, p. 35 s. et 185 s.
[511] Pour une brève présentation de la notion de donnée sensible, v. *Le Lamy droit du numérique*, *V°* « Qu'entend-t-on par données "sensibles" », § 3925, actu. 2020, dir. M. Vivant.
[512] Voir les articles 18, 30, 31 et 32 de la loi n° 78-17 du 6 janv. 1978.

sexuelle[513]. Le règlement européen a étendu encore davantage le domaine des données sensibles en y ajoutant l'orientation sexuelle, les données génétiques et les données biométriques[514]. Dès lors qu'un traitement permet de révéler une information de ce type à l'égard d'une personne[515], la donnée recevra la qualification de « donnée sensible »[516].

143. Une dualité notionnelle favorisant le caractère accueillant de la notion de donnée à caractère personnel. En créant, au sein même de la notion de donnée à caractère personnel, un sous-ensemble de données jugées sensibles[517], les législateurs encouragent une acception large de la simple donnée à caractère personnel. En effet, comme les données à caractère personnel ne se limitent pas à celles intimement liées à la personne (telles que ses opinions religieuses ou son origine ethnique), les interprètes sont invités à faire entrer dans la notion toutes les informations pouvant contribuer à la révélation de la personne, et cela même lorsque le lien est lointain (telles qu'une adresse IP ou des logs de serveurs)[518].

Le noyau dur des données est immanquablement protégé contre les traitements les plus intrusifs[519]. Autour de ce noyau gravite une profusion de simples données à caractère personnel, lesquelles peuvent porter sur des aspects triviaux de la vie des personnes. En n'étant pas limitée aux données étroitement liées à la personne, la notion de donnée à caractère personnel devient alors le réceptacle de toutes les informations entretenant un lien, même très indirect, avec une personne. La reconnaissance de la catégorie de données sensibles favorise donc une interprétation extensive de la simple donnée à caractère personnel. Celle-ci se confirme lors de l'analyse de l'interprétation retenue de la notion de donnée à caractère personnel.

---

[513] Art. 8 de la loi n° 78-17 du 6 janv. 1978 telle que modifiée par la loi n° 2004-801 du 6 août 2004.
[514] Art. 9 du règlement UE n° 2016/679. Un sort particulier est réservé aux données relatives aux infractions dans l'article 10 de ce texte.
[515] Pour une étude de la distinction entre les données sensibles selon leur nature ou le contexte dans lequel elles sont traitées, v. C. Koumpli, *Les données personnelles sensibles. Contribution à l'évolution du droit fondamental à la protection des données à caractère personnel*, th. Paris I, 2019, p. 187 s.
[516] Le considérant 10 du règlement UE n° 2016/679 retient cette expression pour « le traitement de catégories particulières de données à caractère personnel ».
[517] *Le Lamy droit du numérique*, *V°* « Qu'entend-t-on par données "sensibles" », § 3925, actu. 2020, dir. M. Vivant.
[518] Sur la qualification des adresses IP comme des données à caractère personnel, v. *infra*, n^os^ 186 s.
[519] Pour une mise en perspective jurisprudentielle des notions de vie privée et de donnée à caractère personnel, v. *infra*, n^os^ 206 s.

§ II. Le rôle de l'interprète dans l'expansion

144. L'interprétation de la notion. L'exposé de la notion de donnée à caractère personnel, tel qu'elle ressort des textes, donne une impression de clarté. Très simplement, si une donnée se rapporte à une personne, elle doit recevoir la qualification de donnée à caractère personnel. Pourtant, la pratique montre qu'une telle application n'est pas si aisée. Par exemple, une donnée de connexion, une suite aléatoire de chiffres, le pixel d'une photo se rapportent-ils à une personne ? Il est impossible pour le législateur de régler d'avance, par la loi, tous les besoins concrets de la vie juridique. Ainsi, entre la formule rigide de la loi et la réalité des traitements, il faut un intermédiaire qui puisse, et sache, adapter cette formule aux situations et circonstances pour lesquelles elle est écrite[520]. Cet intermédiaire, c'est l'interprète du droit, et en matière de données à caractère personnel, ce rôle est incarné par les autorités de contrôle et les juges.

145. Plan. Les autorités de contrôle ont interprété très largement la notion de donnée à caractère personnel (A), et, malgré des réticences initiales, les juges ont adopté une interprétation large de la notion (B).

A. L'interprétation très large par les autorités de contrôle

146. Plan. La généreuse interprétation de la notion de donnée personnelle retenue par la CNIL (1) se retrouve également dans les travaux du G29, le groupe des autorités de contrôle (2).

1. La contribution de la CNIL à l'expansion de la notion

147. Une interprétation large de la notion d'information nominative. Déjà sous l'empire de la loi du 6 janvier 1978, la CNIL avait retenu une interprétation étendue de la notion d'information nominative. En effet, l'institution considérait qu'elle incluait tous les éléments conduisant à l'identification d'une personne, alors même qu'une lecture littérale de ces termes n'encourageait pas une telle interprétation[521]. La CNIL considérait par exemple que relevait de cette notion : une photographie[522], une liste

[520] F. Gény, *Méthodes d'interprétation et sources en droit privé positif,* t. 1, LGDJ, 1919, n° 85, p. 212.
[521] V. *supra,* n° 138.
[522] CNIL, *Voix, image et protection des données personnelles*, La Documentation française, 1996.

d'abonnés à l'annuaire[523], des factures[524], des photographies d'un immeuble[525]… L'autorité appliquait la notion à tout type d'information, quels que soient la forme des données ou le support utilisé[526].

148. Une interprétation large de la notion de donnée à caractère personnel. L'adoption en droit français de la notion de donnée à caractère personnel a permis à la CNIL de poursuivre, en toute légitimité cette fois, le mouvement entamé. À de nombreuses reprises, la CNIL a continué d'étendre la notion, notamment en 2014, à l'occasion d'une sanction prononcée à l'égard de Google dans laquelle l'institution a affirmé que « les législateurs européen et français ont consacré une conception large de la notion de donnée à caractère personnel [et que] la qualification de données à caractère personnel peut ainsi s'appliquer non seulement à l'adresse IP et aux données collectées par le vecteur des cookies, mais également à tous les types d'identifiants uniques, tels que celui du terminal ou d'un composant du terminal de l'utilisateur, le résultat du calcul d'empreinte dans le cas du *fingerprinting*, ou encore l'identifiant généré par un logiciel ou un système d'exploitation »[527]. Cette délibération identifiait également d'autres types de données à caractère personnel, telles que les termes d'une recherche, la vitesse de frappe de l'utilisateur sur son clavier, sa localisation… Ainsi, en apparence, rien ne semble limiter l'interprétation de la CNIL de la notion de la donnée à caractère personnel.

149. La CNIL, l'autorité des données ? Parfois la CNIL étend de manière excessive la notion de donnée à caractère personnel. Par exemple, l'institution avait un temps considéré que le simple pixel de l'image représentant une personne pouvait être qualifié de donnée indirectement identifiante[528]. Pourtant, ce n'est que la pluralité de pixels qui

---

[523] CNIL, délibération nº 97-060 du 8 juillet 1997 portant recommandation relative aux annuaires en matière de télécommunications.
[524] CNIL, délibération nº 80-016 du 6 mai 1980 concernant les traitements automatisés d'informations nominatives relatifs à la consommation de gaz, d'électricité, d'énergie de toute nature et d'eau et aux redevances d'assainissement facturables par des services publics concédés, affermés, en régie intéressée ou en régie directe.
[525] CNIL, *Rapport d'activité 2002,* La Documentation française, 2003, p. 142.
[526] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés*. *La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 484, p. 213.
[527] CNIL, délibération nº 2013-420 du 3 janvier 2014 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google Inc. V. déjà en ce sens au sujet de l'identifiant d'un téléphone, CNIL, *Rapport d'activité 2008,* La Documentation française, 2009, p. 50.
[528] Selon Monsieur Alain Bauer, la CNIL a considéré que le simple pixel de l'image d'une personne pouvait être qualifié de donnée à caractère personnel, v. Arrêt sur images, « Vidéosurveillance : l'État est un petit joueur par rapport à Facebook », 6 déc. 2013.

rend possible l'identification de la personne[529]. L'institution a également affirmé qu'une base de données contenant des informations relatives à des arbres remarquables contenait des données à caractère personnel[530]. En effet, le pouvoir de recouper ces données avec d'autres informations, telles que celles contenues dans le cadastre[531], permettrait à un tiers d'obtenir des renseignements sur la situation patrimoniale du propriétaire de l'arbre et, à ce titre, relevait donc de la notion de donnée à caractère personnel.

L'engouement de la CNIL pour des sujets liés aux données non personnelles, tels que l'*open data*[532] ou la *blockchain*[533], invite également à se demander si l'autorité ne souhaiterait pas devenir l'institution de référence pour toutes les données. Il est intéressant de remarquer que le Conseil d'État encourage une telle compétence extensive puisqu'il a récemment affirmé « qu'il résulte de l'économie générale de la loi du 6 janvier 1978 (…), que la CNIL est chargée de veiller à la conformité de *tout* traitement de données relevant de son champ d'application, *qu'il concerne ou non des données à caractère personnel* »[534]. Le Conseil d'État retient donc lui aussi une interprétation large de la compétence de la CNIL en matière de données et l'incite à étendre ses contrôles à tous les traitements de données.

Ces exemples illustrent la difficulté des institutions à circonscrire le champ d'application de la notion et celui de la compétence de la CNIL.

2. La contribution du G29 à l'expansion de la notion

150. L'interprétation extensive de la notion de donnée à caractère personnel. Le groupe des autorités de contrôle (G29) institué par la directive 95/46, composé des

---

[529] En appliquant l'entropie de Shannon, c'est-à-dire la fonction mathématique correspondant à la quantité d'information contenue ou délivrée par une source d'information, il est possible de dire qu'un pixel a une grande entropie. En effet, il existe une grande incertitude sur ce que la source émet, et donc sur le caractère identifiant d'un seul pixel pris aléatoirement, v. C. Shannon, « A mathematical theory of communication », *The Bell System Technical Journal* 1948, vol. 27, p. 379. V. aussi, R. Chellappa, P. Sinha et P. Jonathon Philips, « Face recognition by computers and humans », *IEEE Computer Society* 2010, vol. 43, nº 2, p. 46.

[530] Cette affirmation a eu lieu à plusieurs reprises dans des entretiens informels avec des agents de la CNIL lors de la mise à disposition des bases de données concernant les arbres remarquables. Ces arbres sont exceptionnels par leur âge, leurs dimensions, leurs formes, leur passé ou encore leur légende.

[531] Le cadastre est « un ensemble de documents de nature purement administrative (plan cadastral, états de section, matrices cadastrales) établis par la commune qui donnent un état représentatif et évaluatif de la propriété bâtie et non bâtie de la France », G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vº* « Cadastre », sens 1.

[532] V. par ex. les nombreuses pages consacrées à ce sujet dans son rapport d'activité de l'année 2016, CNIL, *Rapport d'activité 2016,* La Documentation française, 2017, p. 30 s. Pourtant l'année 2016 fut marquée par l'adoption de deux textes importants : la loi pour une République numérique et le règlement européen nº 2016/679.

[533] En septembre 2018, c'est-à-dire quatre mois après l'entrée en application du règlement européen, la CNIL a établi un guide relatif à la blockchain, v. CNIL, « Premiers éléments d'analyse de la CNIL. Blockchain », sept. 2018.

[534] CE Sec. 19 juin 2020, nº 434684, *Association des agences-conseils en communication et autres*, § 5, *Lebon T.*

représentants des autorités de protection des États membres, était notamment chargé d'émettre des recommandations sur toute question concernant la protection des données à caractère personnel[535]. Naturellement, le G29 s'est prononcé sur la notion de donnée à caractère personnel, en retenant une acception très large de celle-ci[536]. Il considère que toute information quelles qu'en soient son contenu, sa nature ou son format, peut être qualifiée de donnée à caractère personnel[537]. Le G29 précise d'ailleurs que « l'expression "donnée à caractère personnel" englobe les informations touchant à la vie privée et familiale d'une personne physique, *stricto sensu*, mais également les informations relatives à ses activités, quelles qu'elles soient, tout comme celles concernant ses relations de travail ainsi que son comportement économique ou social »[538]. Le G29 considère aussi que des informations concernant des objets (telles que la valeur d'une maison), des processus ou des évènements (tels que l'entretien automobile) peuvent avoir trait à une personne physique et être qualifiées de données à caractère personnel[539].

151. Pour le G29, les données sont par défaut personnelles. Le groupe retient une interprétation si large de la notion de donnée à caractère personnel qu'il conclut son avis sur ce concept en affirmant qu'il est envisageable « que, *dans certaines circonstances*, les informations ne soient pas considérées comme des données à caractère personnel ». Une telle assertion est le signe d'une vision hégémonique de la notion puisque, par principe, les données sont considérées comme des données à caractère personnel et *exceptionnellement* elles peuvent être non personnelles[540]. Les avis postérieurs du G29 et du Comité Européen de la Protection des Données (CEPD)[541] ont confirmé cette interprétation extensive de la notion[542].

---

[535] Les missions du groupe G29 étaient prévues par l'article 30 de la directive UE nº 95/46.
[536] G29, WP 136, Avis 4/2007 du groupe de travail relatif au concept de données à caractère personnel, 20 juin 2007.
[537] G29, WP 136, Avis 4/2007 du groupe de travail relatif au concept de données à caractère personnel, 20 juin 2007, p. 6 s.
[538] G29, WP 136, Avis 4/2007 du groupe de travail relatif au concept de données à caractère personnel, 20 juin 2007, p. 7.
[539] G29, WP 136, Avis 4/2007 du groupe de travail relatif au concept de données à caractère personnel, 20 juin 2007, p. 10.
[540] Madame Nathalie Métallinos remarquait d'ailleurs que le G29 a adopté une « approche conceptuelle assez absolue de la notion permettant d'étendre quasiment sans limites la notion », N. Métallinos, « La CJUE écarte l'approche téléologique de la notion de donnée à caractère personnel », *CCE* 2018, nº 3, comm. 23. Dans le même sens, v. V.-L. Benabou, « L'extension du domaine de la donnée », *Légicom* 2017, nº 59, p. 3, spéc. p. 5 s. V. aussi *supra,* nºs 125 s.
[541] Le CEPD est le successeur du G29, art. 68 du règlement UE nº 2016/679.
[542] V. not. G29, WP 148, Avis 01/2008 sur les aspects de la protection des données liés aux moteurs de recherche, 4 avr. 2008, p. 6 s. ; G29, WP 171, Avis 02/2010 sur la publicité comportementale en ligne, 22 juin 2010, p. 11 ; G29, WP 185, Avis 13/2011 sur services de géolocalisation des dispositifs mobiles intelligents, 16 mai 2011,

B. L'interprétation large par les juridictions

152. Le positionnement des juridictions. Les juridictions ont été moins sollicitées que les autorités de contrôle dans l'interprétation de la notion de donnée à caractère personnel. Lorsqu'elles étaient saisies de cette question, ont-elles contribué au mouvement d'interprétation engagé par les autorités de protection des données ou ont-elles été plus réservées sur l'application de cette notion ?

153. Plan. Les juridictions nationales interprètent de plus en plus largement la notion de donnée à caractère personnel (1) ; quant à la CJUE, elle retient une interprétation extensive de la notion (2).

1. Une interprétation de plus en plus large par les juges nationaux

154. Une compétence interprétative partagée. Préalablement à toute étude dédiée à l'interprétation juridictionnelle du droit des données à caractère personnel, il est important de souligner que la compétence interprétative de cette matière est partagée entre le juge administratif et le juge judiciaire[543].

155. Une interprétation stricte de la notion d'information nominative. Initialement, les juridictions françaises faisaient preuve de prudence dans l'interprétation de la notion d'information nominative. Elles avaient tendance à en retenir une interprétation littérale, cherchant la présence du nominatif dans l'information. Les informations indirectement liées aux personnes entraient rarement dans cette conception stricte. Par exemple, le Conseil d'État et la Cour de cassation ont considéré qu'un sondage comportant des questions qui demandent aux personnes interrogées ce qu'elles pensent d'une personnalité, ne contient pas d'informations qui s'appliquent à celle-ci[544]. Par ailleurs, le Conseil d'État a également considéré qu'un numéro d'ordre[545] ou des « statistiques récapitulant, pour chacune des auto-écoles du département de la Moselle, d'une part le nombre d'élèves présentés et reçus à l'examen

---

p. 4 s. ; G29, WP 207, Avis 6/2013 sur la réutilisation des informations du secteur public (ISP) et des données ouvertes, 5 juin 2013, p. 15 s.

[543] Sur cette compétence partagée et ses conséquences, v. *infra*, n^os^ 515 s.

[544] CE Sec., 9 juill. 1997, *Chambre Syndicale Syntec Conseil*, n° 148975, *Lebon* p. 301 ; Cass. crim., 12 mai 1998, n° 96-85.900, *Bull. crim*. 1998, n° 158, p. 422. Sur cette question, la CNIL avait retenu une position contraire, v. CNIL, *Rapport d'activité 1993,* La Documentation française, 1994, p. 215 s.

[545] CE Sec., 30 déc. 1998, *Syndicat national des personnels de l'éducation surveillée*, n° 188233, inédit *Lebon*.

du permis de conduire, d'autre part le taux de réussite à cet examen calculé sur la base de ces éléments »[546] ne contenaient aucun élément de caractère nominatif. Les juridictions adoptaient donc une interprétation relativement stricte de la notion d'information nominative.

156. Une interprétation extensive de la notion de donnée à caractère personnel. Le passage de la notion d'information nominative à celle de donnée à caractère personnel a encouragé les juges à abandonner cette interprétation rigoureuse. Après ce glissement, le Conseil d'État a reconnu le caractère personnel à de nombreuses données, notamment aux coordonnées téléphoniques[547], à la localisation d'un bien en vente[548], ou à l'adresse MAC d'un téléphone[549]. La Cour de cassation a rejoint cette interprétation large de la notion[550], puisqu'elle reconnaît un caractère personnel aux données telles que la géolocalisation d'employés[551], l'adresse IP[552] ou les écrits faisant état d'appréciations sur une personne[553]. Ainsi, les juridictions nationales font entrer de nombreuses données dans la notion de donnée à caractère personnel, et cela même lorsqu'elles sont indirectement identifiantes. Cette interprétation accueillante se retrouve aussi dans la jurisprudence de la Cour de justice de l'Union européenne.

2. Une interprétation large par la Cour de justice de l'Union européenne

157. Une interprétation justifiée par la lettre des textes. Selon la Cour de justice, « le champ d'application de la directive 95/46 apparaît très large »[554] et « les données à caractère personnel visées par la directive sont variées »[555]. À partir de ce constat, la CJUE a développé une jurisprudence accueillante pour la notion de donnée à caractère personnel.

---

[546] CE Sec., 3 juill. 2002, *Ministre de l'équipement, des transports et du tourisme*, n° 157402, *Lebon T.* p. 730.
[547] CE réf., 5 sept. 2008, *Société Directannonces*, n° 319071, inédit *Lebon*.
[548] CE réf., 5 sept. 2008, *Société Directannonces*, n° 319071, inédit *Lebon*.
[549] CE Sec., 8 févr. 2017, *JC Decaux France*, n° 393714, *Lebon T.* p. 614.
[550] Souvent, lorsqu'il est saisi, le juge judiciaire a tendance à se référer, en sus des dispositions applicables aux données personnelles, à l'article 9 du code civil, v. not. Cass. civ. 1re, 27 nov. 2019, n° 18-14.675, *Bull. civ.* 2019 ; Cass. civ. 1re, 10 sept. 2014, n° 13-12.464, *Bull. civ.* 2014, I, n° 144, v. sur les liens entre ces deux notions dans la jurisprudence, *infra,* nos 206 s.
[551] Cass. soc., 19 déc. 2018, n° 17-14.631, *Bull. soc.* 2018.
[552] Cass. civ. 1re, 3 nov. 2016, n° 15-22.595, *Bull. civ.* 2016, n° 206, p. 251.
[553] Cass. crim., 8 sept. 2015, n° 13-85.587, *Bull. crim.* 2016, n° 443.
[554] CJCE, 6 nov. 2003, *Bodil Lindqvist*, C-101/01, § 88.
[555] CJCE, 7 mai 2009, *Rijkeboer*, C-553/07, § 59.

158. Variété de données entrant dans la notion de données à caractère personnel. Depuis le début des années 2000, la CJUE a étendu l'application de la notion de donnée à caractère personnel à des informations diverses puisqu'elle comprend les noms[556], les numéros de téléphone ou les informations relatives aux conditions de travail et aux passe-temps[557], les revenus alloués par certaines entités à certains bénéficiaires[558], l'image d'une personne enregistrée par une caméra[559], les données ayant trait à des activités professionnelles[560], la liste des participants à une réunion[561], les données de connexion[562], ou les adresses IP dynamiques[563].

Marquant un certain retrait par rapport à cette interprétation large, la Cour avait considéré, en 2014, que l'analyse juridique figurant dans les minutes d'une décision, même si elle peut contenir des données à caractère personnel, ne constitue pas pour autant, en elle-même, une telle donnée[564]. La CJUE avait fondé cette interprétation sur le fait qu'une telle qualification servirait, en réalité, non pas l'objectif de la directive 95/46, mais celui de l'accès aux documents administratifs garanti par d'autres textes[565]. Madame Nathalie Métallinos avait critiqué cette interprétation qui, selon elle, inscrivait la notion de donnée à caractère personnel dans une approche téléologique[566]. Celle-ci obligerait l'interprète à s'intéresser au contexte dans lequel la donnée est traitée, plutôt que d'avoir une approche statique[567]. La Cour a rapidement renoué avec une approche extensive et *in abstracto* de la notion de donnée à caractère personnel. Elle a ainsi considéré que les réponses écrites fournies par un candidat au cours d'un examen professionnel et les annotations de l'examinateur s'y rapportant constituent des

---

[556] CJUE, 20 déc. 2017, *Peter Nowak* c. *Data Protection Commissioner*, C-434/16, § 29.
[557] Dans sa décision *Lindqvist* la Cour de justice de l'Union européenne estime que la notion « comprend assurément le nom d'une personne joint à ses coordonnées téléphoniques ou à des informations relatives à ses conditions de travail ou à ses passe-temps », puis élargit cette notion en supprimant l'adverbe « joint », CJCE, 6 nov. 2003, *Bodil Lindqvist*, C-101/01, § 24 et § 27.
[558] CJCE, 20 mai 2003, *Rechnungshof*, C-465/00, C-138/01 et C-139/01, § 64.
[559] CJUE, 11 déc. 2014, *František Ryneš* c. *Úřad pro ochranu osobních údajů*, C-212/13, § 22.
[560] CJUE, 9 nov. 2010, *Volker und Markus Schecke GbR* et *Hartmut Eifert*, C-92/09 et C-93/09, § 59.
[561] CJUE, 29 juin 2010, *Commission européenne* c. *Bavarian Lager Co.,* C-28/08, § 70.
[562] CJUE, 8 avril 2014, *Digital Rights Ireland Ltd* c. *Minister for communications et al. et Kärntner Landersregierung*, C-293/12 et C-594/12, § 26 s.
[563] CJUE, 19 oct. 2016, *Patrick Breyer* c. *Bundesrepublik Deutschland*, C-582/14, § 49.
[564] CJUE, 17 juill. 2014, *YS* c. *Minister voor Immigratie, Integratie en Asiel* et *Minister voor Immigratie, Integratie en Asiel* c. *M et S*, C-141/12 et C-372/12, § 38 s.
[565] CJUE, 17 juill. 2014, *YS* c. *Minister voor Immigratie, Integratie en Asiel* et *Minister voor Immigratie, Integratie en Asiel* c. *M et S*, C-141/12 et C-372/12, § 46.
[566] N. Métallinos, « La CJUE écarte l'approche téléologique de la notion de donnée à caractère personnel », *CCE* 2018, nº 3, comm. 23. V. aussi, J. Dupont-Lassalle, « Protection des données personnelles », *Europe* 2014, nº 10, comm. 368. Comp. la proposition formulée par la présente étude, v. *infra*, nºs 271 s.
[567] Selon l'auteur, cette approche statique serait plus protectrice pour les individus.

données à caractère personnel devant être communiquées au titre du droit d'accès protégé[568].

Ainsi, la Cour de justice de l'Union européenne, se fondant sur la volonté du législateur[569], interprète amplement la notion de donnée à caractère personnel, « laquelle n'est pas restreinte aux informations sensibles ou d'ordre privé, mais englobe potentiellement toutes sortes d'informations, tant objectives que subjectives sous forme d'avis ou d'appréciations, à condition que celles-ci "concernent" la personne en cause »[570]. Les juridictions participent également à l'essor de la notion de donnée à caractère personnel. Un tel essor s'explique par une pluralité de causes.

SECTION II – LES CAUSES DE L'ESSOR DE LA NOTION

159. Un droit en mouvement. Le droit est une science dynamique[571], en perpétuel mouvement : il se transforme sans cesse au rythme de l'histoire dont il épouse, freine ou encourage l'évolution, si bien qu'il traduit les conditions de son temps et porte les stigmates de l'époque où il s'est formé[572]. Depuis l'adoption de ses premières règles, le droit des données à caractère personnel a suivi un mouvement d'adaptation, en lien avec les évolutions sociétales et technologiques. Au niveau de la notion de donnée à caractère personnel, objet essentiel à la détermination du domaine de la loi, le mouvement d'expansion est flagrant. Quelles sont les causes ayant contribué à cet essor ?

160. Les relations entre la protection de la vie privée et celle des données personnelles. Le législateur français, conscient des défis pour les libertés individuelles produits par l'informatique, a souhaité garantir le droit au respect de la vie privée face

---

[568] CJUE, 20 déc. 2017, *Peter Nowak* c. *Data Protection Commissioner*, C-434/16, § 42.
[569] Selon la CJUE, « l'emploi de l'expression "toute information" dans le cadre de la définition de la notion de "donnée à caractère personnel", figurant à l'article 2, sous a), de la directive 95/46, reflète l'objectif du législateur de l'Union d'attribuer un sens large à cette notion », CJUE, 20 déc. 2017, *Peter Nowak* c. *Data Protection Commissioner*, C-434/16, § 34.
[570] CJUE, 20 déc. 2017, *Peter Nowak* c. *Data Protection Commissioner*, C-434/16, § 34.
[571] Les débats sur le droit comme technique ou comme science sont anciens, v. not. H. Lévy-Bruhl, « La science du droit ou "juristique" », *Cahiers Internationaux de Sociologie* 1950, vol. 8, p. 123. Pour Jean Carbonnier, « toute science systématise ; mais le droit, sous un certain aspect, semble n'être que cela. Les sources formelles font connaître les règles de droit dans la dispersion et parfois l'incohérence (même la synthèse que tente une codification peut n'être pas satisfaisante), avec des doubles emplois et, à l'inverse, des lacunes. Il faut classer, rassembler, compléter ou éventuellement éliminer, bref mettre en ordre, imprimer aux dispositions particulières l'unité d'un système », J. Carbonnier, *Droit civil,* vol. 1, *Introduction. Les personnes. La famille, l'enfant, le couple*, PUF, 2004, n° 23, p. 54 s.
[572] J.-L. Bergel, *Théorie générale du droit*, 5e éd., Dalloz, 2012, n° 97, p. 124.

aux évolutions technologiques[573]. Pour cela, il a notamment adopté des règles spécialement dédiées aux traitements des données personnelles, indépendantes de celles relatives au droit au respect de la vie privée. Une telle indépendance n'a-t-elle pas favorisé l'essor de la notion de donnée à caractère personnel ?

161. L'évolution des technologies. En plus de cette distinction de fondements, la volonté de protéger la personne dans toutes ses dimensions, tant dans les éléments liés à son identité[574] que dans ceux composant sa personnalité[575], ont eu des effets sur la notion de donnée à caractère personnel. Il est vrai que les technologies modernes permettent de se faire une idée de plus en plus précise sur les personnes grâce aux traces qu'elles laissent à l'occasion de leur activité en ligne et hors ligne[576]. Cette évolution des méthodes d'identification n'est-elle pas l'une des justifications invoquées pour étendre la notion de donnée à caractère personnel ? Par ailleurs, l'augmentation des acteurs soumis au droit des données à caractère personnel n'a-t-elle pas eu tendance à engendrer des difficultés dans son application ?

162. Plan. De nombreuses causes expliquent le mouvement d'expansion de la notion de donnée à caractère personnel. Parmi celles-ci figurent assurément la dualité de fondement protégeant les informations relatives aux personnes (§ I), les avancées technologiques (§ II), ainsi que les difficultés liées à l'application du droit des données à caractère personnel (§ III).

§ I. L'autonomisation du droit des données à caractère personnel par rapport au droit au respect de la vie privée

163. Plan. Les constructions juridiques de la protection de la vie privée et des données personnelles sont complémentaires : elles visent toutes deux la protection

---

[573] Comme en témoigne le rapport Tricot qui se proposait « de régler la circulation automatisée des données » dans la mesure « nécessaire à la protection de la vie privée », B. Tricot, « Rapport de la commission Informatique et libertés », La Documentation française, 1975, p. 45.

[574] Sur la distinction entre identité classique et identité numérique, v. E. Netter, *Numérique et grandes notions du droit privé. La personne, la propriété, le contrat*, mémoire en vue de l'habilitation à diriger des recherches en droit privé, Picardie, 20 nov. 2017, n^{os} 28 s., p. 47. Sur la personnalité numérique, v. B. Gleize, « La personnalité numérique », in *Mélanges M. Vivant,* Dalloz, 2020, p. 189 s., spéc. p. 192.

[575] J. Rochfeld, « La vie tracée ou le code civil doit-il protéger la présence numérique des personnes ? », in *Mélanges J. Hauser*, LexisNexis et Dalloz, 2012, p. 619 s., n^{o} 11, spéc. p. 631.

[576] Sur le fait que les traces sont consubstantielles à l'usage des technologies, v. déjà J. Frayssinet, « La traçabilité des personnes sur l'internet », *Dr et pat.* 2001, n^{o} 93, p. 38.

d'informations relatives à une personne physique (A). En dépit de cette complémentarité, les deux protections sont fondées sur des principes juridiques distincts, propices à une disjonction entre les notions (B).

A. Des constructions complémentaires

164. Histoire de la protection de la vie privée. La construction de la protection juridique de la vie privée ne s'inscrit pas dans un déroulement linéaire et intelligible[577] ; en réalité, ce sont plutôt « des » histoires plurielles de la vie privée qui coexistent. D'autant que différentes conceptions de la vie privée sont engendrées par les sociétés dans lesquelles elles se développent[578]. En France, la protection juridique de la vie privée a suivi plusieurs mouvements et est passée d'une protection sectorielle à une protection d'ensemble. L'adoption en 1970 d'une loi reconnaissant un droit général au respect de la vie privée a constitué le paroxysme de cette protection juridique.

165. Histoire de la protection des données personnelles. Contrairement à la protection de la vie privée, la construction juridique du droit des données personnelles est assez linéaire, plutôt singulière. Elle émerge beaucoup plus récemment puisqu'elle apparaît avec les développements de l'informatique[579]. Dans les démocraties occidentales, l'objet de cette matière vise à garantir une protection de la vie privée, en dépit de l'informatisation de la société[580]. Si la protection de la vie privée s'est construite de manière erratique, par des reconnaissances progressives et sectorielles, le droit des données personnelles a été élaboré dans un but déterminé et avec un objet identifié.

166. Un objectif commun. L'analyse des constructions historiques de ces deux protections aide à mieux appréhender les interactions entre ces législations. Elles

---

[577] J. Mourgeon, *Les droits de l'homme*, 8e éd., PUF, 2008, p. 19.
[578] X. Bioy, « Le libre développement de la personnalité en droit constitutionnel, essai de comparaison Allemagne, Espagne, France, Italie, Suisse », *RID comp.* 2003, vol. 55, nº 1, p. 123, spéc. p. 125 s. Plus généralement sur les inspirations historiques à la reconnaissance des droits de l'homme, v. S. Hennette-Vauchez et D. Roman, *Droits de l'Homme et libertés fondamentales*, 4e éd., Dalloz, 2020, nos 43, p. 47 s.
[579] V. not. A. Westin, *Privacy and Freedom*, Ig Publishing, 1968, réimpr. 2015, p. 3.
[580] V. not. les travaux conduits par l'OCDE à la fin des années 1960 relatifs à l'informatique et aux télécommunications, OCDE, « Rapport sur la table ronde sur le recours à l'informatique pour les travaux parlementaires », nº 4312, 23 avr. 1979, p. 4. Sur la convergence initiale entre le droit au respect de la vie privée et le droit des données personnelles, v. D. Lindsay, « The relationship between general law protection of privacy and information privacy laws », in *Personal data & privacy protection*, dir. A. Saad, LexisNexis, 2005, p. 29.

partagent un point commun essentiel : celui de protéger des informations en lien avec des personnes physiques.

167. Plan. Une analyse concise des mouvements historiques ayant conduit à l'adoption de la protection juridique de la vie privée (1) et de celle des données à caractère personnel (2) permet de mieux comprendre la complémentarité de ces législations.

1. La construction historique de la protection de la vie privée

168. Les origines. En France, trois domaines liés à la vie privée ont historiquement été protégés : le domicile[581], les correspondances[582] et les informations personnelles divulguées par la presse[583]. En sus des lois spécifiquement consacrées à ces protections, le code civil a encadré les vues sur la propriété de son voisin[584], la publicité du contrat

[581] En France, la protection du domicile est reconnue depuis le décret sur la police municipale et correctionnelle du 19 juillet 1791. Cette protection juridique du domicile prend, en Occident, ses racines dans les textes religieux. Le livre de l'Exode de la Bible prévoit en effet dans son verset 22:2 que « Si le voleur est surpris dérobant avec effraction, et qu'il soit frappé et meure, on ne sera point coupable de meurtre envers lui ». Le meurtre du voleur qui cherche à pénétrer pendant la nuit dans une maison « en brisant la porte ou en perçant une muraille » est donc toléré. Le Talmud offre un éclairage intéressant de cette règle puisqu'il explique que les individus protègent la propriété de leur maison et le voleur qui s'introduit dans une maison doit être prêt à être tué par son propriétaire. On lit également dans le Coran : « Ô croyants ! N'entrez pas dans une maison étrangère sans en demander la permission et sans saluer ceux qui l'habitent. Si vous n'y trouvez personne, n'entrez pas, à moins qu'on ne vous l'ait permis ». Pour une étude historique de la protection du domicile, v. C. Arminjon, *Étude sur les droits du particulier dans son domicile et sur les restrictions que ces droits subissent dans l'intérêt public*, th. Dijon, 1900, p. 15. Pour des études plus récentes de la protection du domicile, v. not. I. Gravelais, *La protection juridictionnelle de l'inviolabilité du domicile,* th. Dijon, 2013 ; G. Dumenil, *Le domicile en droit pénal,* th. Paris II, 2017.

[582] Le principe de l'inviolabilité de la correspondance n'était inscrit formellement dans aucune loi constitutionnelle ni dans la Déclaration des droits de l'homme et du citoyen. Cependant, il résulte de l'esprit et des grands principes révolutionnaires, notamment du principe proclamé par l'article 11 de la Déclaration des droits de l'homme de 1789. C'est en 1810, avec l'article 187 du code pénal, qu'il devient en droit français une règle incontestée. Malgré cette consécration, il faudra attendre plusieurs décennies avant que la pratique ne s'aligne sur les principes juridiques, v. Y. M. Danan, *Histoire postale et libertés publiques*, LGDJ, 1965, p. 66 s.

[583] C'est principalement à l'égard des divulgations dans la presse que la vie privée s'est développée, notamment dans des lois de 1819, 1868 et 1881. V. loi du 17 mai 1819 sur la répression des crimes et délits commis par la voie de la presse, ou par tout autre moyen de publication, *B.* 278 nº 6444 ; loi du 26 mai 1819, *Moniteur Universel*, 14 juin 1819, p. 782, nº 165 ; loi du 9 juin 1819, *B.* 284, nº 6648 et 6649. Si la notion de vie privée n'apparaît pas explicitement dans les termes de ces lois, elle était l'objet de discussions au Parlement, notamment dans le discours du député Royer-Collard du 27 avril 1819. V. aussi la loi nº 15-979 du 11 mai 1868 relative à la presse, *D.* 1868, IV, p. 62 dont l'article 11 prévoyait que « Toute publication dans un écrit périodique relative à un fait de la vie privée constitue une contravention punie d'une amende de cinq cent francs. La poursuite ne pourra être exercée que sur la plainte de la partie intéressée ». Dans sa version initiale, la loi du 29 juillet 1881 sur la liberté de la presse (*JORF* 30 juill. 1881, nº 206, p. 4201) ne faisait pas mention de la vie privée et s'inscrivait donc en rupture avec les développements législatifs précédents, v. J.-L. Halpérin, « L'essor de la "privacy" et l'usage des concepts juridiques », *Droit et Société* 2005, nº 61, p. 765 s., spéc. p. 772. Il a fallu attendre l'ordonnance du 6 mai 1944 pour que le législateur reprenne ce terme, v. ordonnance du 6 mai 1944 relative à la répression des délits de presse, *JORF* 20 mai 1944, nº 0042, p. 402.

[584] P. Kayser, « Le secret de la vie privée et la jurisprudence civile », in *Mélanges R. Savatier*, Dalloz, 1965, p. 405 s., nº 1, spéc. p. 405, citant les articles 675 à 680 du code civil. Cette limite peut s'assimiler à la protection du domicile contre les intrusions de tiers.

de mariage[585], et a interdit la reproduction par voie de presse des débats de l'instance du divorce[586]. Ces protections par « bulles » permettaient de poser un voile sur l'intimité des personnes[587], contribuant ainsi à leur libre expression personnelle dans leur domicile et dans leurs correspondances[588].

169. Le développement de la protection de la vie privée sur le fondement de la responsabilité civile. Ces fondements spécifiques protégeant certains aspects de la vie privée des personnes étaient insuffisants pour encadrer l'ensemble des atteintes subies par les victimes de divulgations et d'investigations dans leur vie privée[589]. Aussi ces victimes ont invoqué, devant les juridictions civiles, le bénéfice de la responsabilité délictuelle pour protéger de nombreuses informations les concernant[590]. Parce que les atteintes à la vie privée sont si particulières, les juges avaient adapté deux des trois conditions de cette responsabilité, c'est-à-dire la faute et le préjudice[591]. Ils ont ainsi opéré un glissement sur la caractérisation de ces conditions et ont accueilli des actions en responsabilité, alors même que les requérants ne rapportaient pas toujours la preuve de ces trois conditions. Ainsi, le seul fait de divulguer des éléments de la vie privée d'une personne est progressivement considéré comme une faute et la preuve du préjudice devient de moins en moins essentielle[592].

---

[585] Loi du 17 juin, 2 et 10 juillet 1850 sur la publicité des contrats de mariage, *Le Conservateur* 31 août 1850, 4e année, no 2.
[586] Loi du 18 avril 1886 sur la procédure en matière de divorce et de séparation de corps, *JORF* 20 avr. 1886. L'article 1er de cette loi modifiait l'article 239 du code civil.
[587] Dans plusieurs discours, le député Royer-Collard évoquait la métaphore du mur entourant la vie privée. Ainsi, selon lui, « il n'est pas permis de dire la vérité sur la vie privée. Voilà la disposition principale, le reste est une exception… Voilà donc la vie privée murée, si je puis me servir de cette expression ; elle est déclarée invisible, elle est renfermée dans l'intérieur des maisons », P.-P. Royer-Collard, *De la liberté de la presse*, Librairie de Médicis, 1949, p. 24 s.
[588] Une telle liberté ne peut exister que si la personne n'a pas peur de voir divulguer ses attitudes ou confidences auprès de tiers. Madame Muriel Fabre-Magnan s'interrogeait justement sur les effets de la surveillance numérique pour la liberté personnelle : « sommes-nous vraiment libres lorsque la surveillance numérique est presque totale, lorsque nombre de données les plus personnelles sont enregistrées, conservées, diffusées à tous, enfermant chaque personne dans un "profil" figé dont la traçabilité sera généralisée ? », M. Fabre-Magnan, *L'institution de la liberté*, PUF, 2018, p. 13. Le développement individuel ne peut exister en l'absence d'espaces personnels, tel que l'a décrit Virginia Wolf dans son essai *Une chambre à soi*, v. *supra*, no 4. Ce besoin se retrouve aussi dans une citation de Winston Churchill selon qui « tout prophète doit venir de la civilisation, mais tout prophète doit aller dans le désert. Il faut qu'il soit profondément imprégné de ce qu'est une société complexe et de tout ce qu'elle a à offrir, et ensuite il faut qu'il passe par des périodes d'isolement et de méditation. C'est par ce processus que se fabrique la dynamique psychique ». V. aussi, J. Cohen, « What privacy is for », *Harvard Law Review* 2013, vol. 126, p. 1904 s. [126 HARV. L. REV. 1904], spéc. p. 1905 et p. 1911.
[589] P. Kayser, « Aspects de la protection de la vie privée dans les sociétés industrielles », in *Mélanges G. Marty*, Université des sciences sociales de Toulouse, 1978, p. 725 s., no 14, spéc. p. 739 ; F. Terré et D. Fenouillet, *Droit civil. Les personnes*, 8e éd., Dalloz, 2012, no 108, p. 118.
[590] Sur la variété des informations protégées sur le fondement de la vie privée, B. Teyssié, *Droit des personnes*, 21e éd., LexisNexis, 2019, nos 165 s., p. 156 s. ; *Rép. civ.* Dalloz, *Vo* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), nos 60 s.
[591] V. *infra*, no 321.
[592] F. Terré et D. Fenouillet, *Droit civil. Les personnes*, 8e éd., Dalloz, 2012, no 108, p. 118.

170. L'adoption de la loi du 17 juillet 1970. Pour contrer cette évolution jurisprudentielle, le législateur français a consacré un fondement propre à la protection de la vie privée avec la loi du 17 juillet 1970[593]. L'économie de cette loi comprend deux parties, l'une introduite dans le code civil, l'autre dans le code pénal[594]. L'article 9 du code civil, dont l'alinéa premier est rédigé en forme de maxime[595], dispose depuis 1970 que :

> « Chacun a droit au respect de sa vie privée.
> Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée ; ces mesures peuvent, s'il y a urgence, être ordonnées en référé ».

171. L'apparente absence de lien entre la protection de la vie privée et les évolutions informatiques. Les débats législatifs ainsi que la protection résultant de la loi de 1970 n'ont pas envisagé les potentiels effets des développements de l'informatique sur la vie privée[596]. Le Parlement avait pourtant examiné, à cette époque, plusieurs projets et propositions de lois visant justement à protéger les informations relatives aux personnes des traitements informatiques[597].

L'apparente indifférence du législateur du 17 juillet 1970 doit être relativisée puisque l'article 9 du code civil fixe une maxime générale. En effet, certains concepts juridiques sont intentionnellement laissés dans le vague parce que l'indétermination intrinsèque de leur contenu est un facteur d'adaptation du droit[598]. Ces textes accordent alors un large pouvoir d'interprétation au magistrat, lui permettant d'adapter ses

---

[593] Loi nº 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens, *JORF* 19 juill. 1970, nº 0166, p. 6755.
[594] M. Contamine-Raynaud, « Le secret de la vie privée », in *L'information en droit privé : travaux de la conférence d'agrégation*, dir. P. Lagarde et Y. Loussouarn, LGDJ, 1978, p. 410. En matière pénale, ce sont notamment les articles 226-1 et suivants du code pénal qui prohibent l'espionnage audio et visuel dans l'intimité de la vie privée.
[595] P. Malaurie et L. Aynès, *Cours de droit Civil,* t. 2, *Les Personnes, les incapacités*, 5e éd., Cujas, 1999, nº 314.
[596] La conception de la vie privée en 1970 restait fortement liée aux atteintes par voie de presse. Le législateur avait proclamé ce droit suite à une demande de plus en plus insistante de la doctrine, v. not. R. Badinter, « Le droit au respect de la vie privée », *JCP G* 1968, I, doctr. 2136.
[597] V. not. la proposition de loi de Michel Poniatowski tendant à la création d'un comité de surveillance et d'un tribunal de l'informatique, Assemblée nationale, nº 1454, déposée le 25 nov. 1970, ainsi que les travaux liés aux lois adoptées, telles que la loi relative à la circulation routière et celle portant réforme hospitalière, v. *infra*, nº 175.
[598] Dans son *Discours préliminaire,* Portalis déclarait d'ailleurs que « l'office de la loi est de fixer, par de grandes vues, les maximes générales du droit : d'établir des principes féconds en conséquences, et non de descendre dans le détail des questions qui peuvent naître sur chaque matière », J.-É.-M. Portalis, *Discours préliminaire au premier projet de Code civil*, Confluences, 1999, p. 17. V. aussi, G. Cornu, *Droit civil. Introduction. Les personnes. Les biens*, 11e éd., Montchrestien, 2003, nº 188, p. 85.

dispositions aux évolutions de la société. La formule de l'article 9 du code civil octroie immanquablement un tel pouvoir au juge, lequel est invité à sanctionner les différentes formes d'atteintes à la vie privée, notamment celles résultant des techniques de transmission et de stockage de l'information propres à l'informatique et aux réseaux[599].

172. L'absence de définition légale de la notion de vie privée. En 1970, le législateur français n'a pas défini, positivement ou négativement[600], la notion de vie privée. Il s'était également abstenu de dresser une liste des éléments protégés, laissant le soin au juge d'en découvrir les domaines[601]. L'étude de la jurisprudence montre le bien-fondé de ce choix puisque cette notion a évolué pour inclure de nombreuses informations relatives aux personnes[602]. Ainsi, elle inclut notamment des éléments tenant à l'identité[603], à la vie familiale[604] et conjugale[605], aux sentiments[606], à la

---

[599] I. Falque-Pierrotin, « Rapport de la mission interministérielle sur l'Internet. "Internet, enjeux juridiques" », La Documentation française, 1997, p. 36. Pour une opinion contraire, considérant que l'article 9 du code civil est une « disposition générale insuffisante pour protéger contre les risques que représente pour les libertés individuelles le traitement informatisé des données nominatives », v. I. de Lamberterie, « Informatique, libertés et opinions religieuses », *Archives des sciences sociales des religions* 1995, vol. 91, n° 1, p. 21.

[600] Certains auteurs ont parfois défini la vie privée par opposition à la vie publique, v. not. L. Martin, « Le secret de la vie privée », *RTD Civ.* 1959, p. 225, n° 3 ; R. Badinter, « Le droit au respect de la vie privée », *JCP G* 1968, I, doctr. 2136, n° 12 ; v. aussi R. Lindon, « La presse et la vie privée », *JCP G* 1965, I, doctr. 1887. Comp. F. Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, Bruylant, 1990, n° 647, p. 724 s.

[601] La CEDH reconnait d'ailleurs qu'il n'est ni possible, ni nécessaire de chercher à définir de manière exhaustive la notion de vie privée, v. not. CEDH, 16 décembre 1992, *Niemietz* c. *Allemagne*, n° 13710/88, § 29 ; CEDH, 25 mars 1993, *Costello-Roberts* v. *Royaume-Uni*, n° 13134/87, § 36.

[602] Pour un exposé des informations relevant de la vie privée, v. F. Terré et D. Fenouillet, *Droit civil. Les personnes*, 8e éd., Dalloz, 2012, n° 109, p. 119 ; *Rép. civ.* Dalloz, *V°* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), nos 71 s.

[603] Cass. civ. 1re, 13 févr. 1985, n° 84-11.630, *Bull. civ.* 1985, I, n° 64, p. 61. Elle inclut le droit au nom (entendu comme l'appellation qui sert à désigner une personne dans la vie sociale), v. J.-M. Plazy, « Le droit au nom », in *Droits de la personnalité,* dir. J.-C. Saint-Pau, LexisNexis, 2013, n° 734, p. 471. Sur l'utilisation des noms et prénoms d'une personne dans un film, Cass. civ. 1re, 13 févr. 1985, n° 84-11.630, *Bull. civ.* I, n° 64, p. 61. Cette protection implique nécessairement le droit à l'anonymat, v. not. J. Pousson-Petit, « Le droit à l'anonymat », in *Mélanges L. Boyer*, PU Toulouse, 1996, p. 595 s., spéc. p. 596 ; J.-C. Saint-Pau, *L'anonymat et le droit*, th. Bordeaux IV, 1998, n° 617. De même, « l'ancienne identité de celui qui a fait légalement changer son nom est un élément de sa vie privée », Cass. civ. 1re, 7 mai 2008, n° 07-12.126, *Bull. civ.* 2008, I, n° 126. Ce droit à l'identité inclut également la protection du droit d'utiliser des pseudonymes, CA Montpellier, 3e ch., 29 sept. 2011, n° 14/04529.

[604] Cass. civ. 2e, 26 nov. 1975, n° 74-12.957, *Bull. civ.* 1975, II, n° 316, p. 253 ; Cass. civ. 1re, 3 avr. 1984, n° 82-15.849, *Bull. civ.* 1984, I, n° 125, p. 103 ; Cass. civ. 1re, 12 juill. 2005, n° 04-11.068, *Bull. civ.* 2005, I, no330, p. 273 ; Cass. civ. 1re, 27 févr. 2007, n° 06-10.393, *Bull. civ.* 2007, I, n° 85, p. 73. La Cour de cassation a considéré que la maternité fait partie de la vie privée, Cass. civ. 2e, 5 janv. 1983, n° 81-13.374, *Bull. civ.* 1983, II, n° 4, p. 3. Elle a aussi considéré que la présentation dans une œuvre romanesque de la disparition d'un couple et de ses enfants constituait une atteinte à leur vie privée, Cass. civ. 1re, 9 juill. 2003, n° 00-20.289, *Bull. civ.* 2003, I, n° 172, p. 134.

[605] Cass. civ. 1re, 13 févr. 1985, n° 84-11.524, *Bull. civ.* 1985, I, n° 63, p. 60. Cela inclut également l'existence d'une vie extraconjugale, CA Paris, 5 mars 1990, *D.* 1990, p. 104 ; ou d'une situation de concubinage, Cass. civ. 1re, 6 oct. 1998, n° 96-13.600, *Bull. civ.* 1998, I, n° 247, p. 191.

[606] Cass. Civ. 1re, 5 nov. 1996, n° 94-14.798, *Bull. civ.* 1996, I, n° 378, p. 265 ; Cass. civ. 1re, 7 févr. 2006, n° 04-10.941, *Bull. civ.* 2006, I, n° 59, p. 649 ; les sentiments incluent la conduite des époux, Cass. civ. 2e, 26 nov. 1975, n° 74-12.957, *Bull. civ.* 1975, II, n° 316, p. 254 ; les relations intimes entretenues par une jeune femme avec un sportif de renom, Cass. civ. 2e, 24 avr. 2003, n° 01-01.186, *Bull. civ.* 2003, II, n° 114, p. 98.

filiation[607], à l'état de santé[608], à la pratique religieuse[609].

En retenant une interprétation dynamique de la notion de vie privée, la jurisprudence étend continuellement son domaine. L'article 9 du code civil abrite ainsi d'autres éléments liés à la personne[610] tels que son image[611] ou sa voix[612], à tel point que plusieurs auteurs l'ont qualifié de « matrice » des droits de la personnalité[613]. Ainsi, la notion de vie privée couvre de nombreuses informations se rapportant aux personnes[614].

2. La construction historique de la protection des données à caractère personnel

173. Les alertes des ingénieurs informatiques. Formidable outil de collecte, d'indexation et d'analyse, l'ordinateur a contribué à l'informatisation des données et à

---

[607] Cass. civ. 1re, 7 nov. 2018, nº 17-25.938, *Bull civ.* 2018. La Cour de cassation a aussi considéré comme une atteinte à la vie privée, l'utilisation d'un enfant et l'exploitation de sa filiation pour lui faire tenir des propos imaginaires ou caricaturaux, Cass. civ. 1re, 20 mars 2014, nº 13-16.829, *Bull. civ.* 2014, I, nº 57, p. 56. V. aussi sur l'interruption volontaire de grossesse qui relève du domaine de la vie privée, CEDH, 20 mars 2007, *Tysiąc* c. *Pologne*, nº 5410/03.

[608] Cass. civ. 2e, 10 juin 2004, nº 02-12.926, *Bull. civ.* 2004, II, nº 292, p. 246. L'intimité de l'existence quotidienne de personnes handicapées relève de leur vie privée, Cass. civ. 1re, 24 févr. 1993, nº 91-13.587, *Bull. civ.* 1993, I, nº 87, p. 57.

[609] Cass. crim., 28 févr. 1874, *Bull. crim.* 1874, II, nº 69, p. 123. Dans cet arrêt historique, la Cour de cassation proclame que « la protection assurée à la vie privée s'étend […] aux actes qui se révèlent extérieurement, s'ils sont du domaine du for intérieur et s'ils intéressent la liberté de conscience ». La Cour de cassation avait considéré que l'envahissement dans la vie privée est caractérisé lorsque le journaliste signale au public les noms des pèlerins qui se sont bornés à se rendre à un pèlerinage, en suivant l'inspiration de leur conscience et sans attirer d'ailleurs par aucun autre acte personnel l'attention du public. Pour un arrêt plus récent, Cass. civ. 1re, 6 mars 2001, nº 99-10.928, *Bull. civ.* 2001, nº 60, p. 39.

[610] Sur l'extension progressive de la protection de l'article 9 du code civil, v. not. J.-M. Bruguière, « Dans la famille des droits de la personnalité, je voudrais », *D.* 2011, p. 28 ; J.-C. Saint-Pau, « L'article 9 du Code civil : matrice des droits de la personnalité », *D.* 1999, p. 541 ; A. Lepage, « L'article 9 du code civil peut-il constituer durablement la "matrice" des droits de la personnalité ? », *Gaz. Pal.* 2007, nº 139, p. 43.

[611] V. not. C. Deschanel, *Le droit patrimonial à l'image : émergence d'un nouveau droit voisin du droit d'auteur*, th. Aix-Marseille, 2017, nos 117 s., p. 95 s. La Cour de cassation a reconnu très tôt le droit d'une personne sur son image, v. not. Trib. Seine, 16 juin 1858, *Rachel*, *D.* 1858, III, p. 62. La jurisprudence protégeant le droit à l'image des personnes a fait l'objet de développements importants, souvent sur le fondement de l'article 9 du code civil, bien qu'il soit désormais établi que le respect dû à la vie privée et celui dû à l'image constituent des droits distincts, v. not. Cass. civ. 1re, 10 mai 2005, nº 02-14.730, *Bull. civ.* 2005, I, nº 206, p. 175. Pour autant, les deux droits restent liés et la Cour de cassation a considéré qu'une « photographie représentant une future mariée allongée et entourée de femmes examinant son hymen pour vérifier sa virginité, constituait une atteinte à la vie privée de cette jeune fille », v. Cass. civ. 2e, 18 déc. 2003, nº 00-22.249, *Bull. civ.* 2003, II, nº 403, p. 333. La Cour de cassation protège de manière stricte le droit à l'image des mineurs, v. not. Cass. civ. 1re, 12 déc. 2000, nº 98-21.311, *Bull. civ.* 2000, I, nº 322, p. 209 ; y compris des enfants de célébrités, v. not. Cass. civ. 2e, 18 déc. 2003, nº 00-22.249, *Bull. civ.* 2003, II, nº 403, p. 333.

[612] Sur la question des formes de protection de la voix, v. D. Huet-Weiller, « La protection juridique de la voix humaine », *RTD civ.* 1982, p. 497, qui distingue la protection de la voix par le droit d'auteur et par le droit au respect de la vie privée.

[613] J.-C. Saint-Pau, « L'article 9 du Code civil : matrice des droits de la personnalité », *D.* 1999, p. 541 ; A. Lepage, « L'article 9 du code civil peut-il constituer durablement la "matrice" des droits de la personnalité ? », *Gaz. Pal.* 2007, nº 139, p. 43.

[614] Selon certains auteurs, la notion de vie privée devient « un concept attrape-tout », il s'agirait même d'une « notion terriblement floue et donc extensible à l'infini, au gré des politiques juridictionnelles », v. P.-Y. Gautier, « La preuve hors la loi ou comment, grâce aux nouvelles technologies, progresse la "vie privée" des salariés », *D.* 2001, p. 3148.

leur enregistrement automatique[615]. Dès les années 1960, les ingénieurs informatiques se sont inquiétés des dangers de cette numérisation pour la protection de la vie privée[616]. Par exemple, le scientifique Bertrand Benson alertait en 1961 sur le fait que la vie privée et les libertés seraient « à la merci de la personne qui appuie sur le bouton pour que la machine enregistre » ces informations[617]. En décembre 1962, le mathématicien Richard Hamming expliquait que le nombre croissant d'informations collectées associé aux capacités de traitement des ordinateurs allaient profondément modifier la conception de la vie privée[618]. La réalité des risques dénoncés par ces ingénieurs s'est matérialisée par plusieurs scandales qui étaient liés à des intrusions dans la vie privée effectuées par les gouvernements.

174. Les scandales des années 1970, témoins de la réalité des risques. Aux États-Unis, plusieurs initiatives du gouvernement fédéral avaient attiré l'attention de la presse et du grand public sur les dangers, pour les libertés individuelles, de la collecte et de l'utilisation des données personnelles. L'une de ces initiatives entendait regrouper dans un système unique ce qui était alors éparpillé entre une vingtaine de systèmes d'information. Le journaliste Vance Packard[619] avait dénoncé ce projet dans le célèbre article du New York Times *Don't tell it to the computer*[620]. Quelques années plus tard, le scandale du Watergate ébranlait la société américaine et avait d'importants échos à l'international. Ce scandale matérialisait la réalité des risques liés aux techniques de surveillance et leurs implications pour la démocratie[621].

---

[615] Pour une étude de la notion de donnée à caractère personnel sous l'angle de l'informatique, v. J. Rossi, *Protection des données personnelles et droit à la vie privée : enquête sur la notion controversée de « donnée à caractère personnel »*, th. Compiègne, 2020, p. 177.

[616] A. Westin, *Privacy and Freedom*, Ig Publishing, 1968, réimpr. 2015, p. 334. Aujourd'hui encore les auteurs rappellent que « le développement de l'informatique affecte directement la vie privée, car les données à caractère personnel – on dit aussi les informations nominatives – permettent l'identification des personnes auxquelles elles s'appliquent et facilitent de manière dangereuse la révélation individuelle ou par interconnexion, des éléments de la vie privée de chacun, de son intimité, de son identité », v. F. Terré et D. Fenouillet, *Droit civil. Les personnes*, 8e éd., Dalloz, 2012, no 118, p. 134.

[617] G. González Fuster, *The emergence of personal data protection as a fundamental right of the EU*, Springer, 2014, p. 29, paraphrasant Bernard Benson.

[618] F. Lane, *American privacy : the 400-year history of our most contested right*, Beacon Press, 2009, p. 144 s., détaillant les interventions de Richard Hamming qui expliquait qu'un nombre croissant d'agences fédérales et d'entreprises utilisaient des ordinateurs pour conserver, suivre et analyser les données relatives aux citoyens. À titre d'exemple il citait l'administration de la Sécurité sociale, le système de sélection pour le service militaire, le service intérieur de l'impôt (*Internal Revenue Service*) et de nombreuses compagnies d'assurances, employeurs, hôpitaux, cabinets médicaux, et compagnies aériennes.

[619] Vance Packard se penchait sur ces problématiques depuis plusieurs années, puisqu'il avait déjà publié, en 1964, *The naked society*, livre alertant sur les risques du développement des technologies pour la protection de la vie privée.

[620] V. Packard, « Don't tell it to the computer », *The New York Times* 8 janv. 1967, p. 236.

[621] H. P. Gassmann, « Vers un cadre juridique international pour l'informatique et les autres techniques nouvelles de l'information », *Annuaire français de droit international* 1985, vol. 31, p. 747, spéc. p. 749.

Quelques années plus tard, des scandales similaires envahissaient la presse française. En 1974, le journaliste Philippe Boucher, alerté par des informaticiens du ministère de l'Intérieur, révélait le projet de centralisation des fichiers personnels dans son illustre article : « "Safari" ou la chasse aux Français »[622]. Ce scandale faisait suite à « l'affaire des plombiers », dans laquelle le ministre de l'Intérieur, Raymond Marcellin, était suspecté d'avoir fait installer des micros espions dans les locaux du *Canard enchaîné*[623]. Les conséquences de ces révélations furent sans appel : abandon du projet SAFARI et nomination d'une commission chargée de proposer des mesures pour garantir le respect de la vie privée et des libertés face au développement de l'informatique[624].

Des scandales de ce type se retrouvent dans de nombreux pays[625]. En Suisse par exemple, l'affaire des fiches avait soulevé des contestations similaires et ébranlé la confiance des citoyens à l'égard de leurs gouvernants, encourageant la mise en place de règles de protection des données plus rigoureuses[626].

175. L'adoption d'une législation « Informatique et libertés ». Avec ces scandales, les travaux concernant l'impact de l'informatique sur les libertés se sont accélérés[627]. Ces travaux n'étaient pas propres à la France puisque d'autres pays discutaient ou adoptaient des législations relatives à la protection des informations

[622] P. Boucher, « 'Safari' ou la chasse aux Français », *Le Monde* 21 mars 1974, p. 9. Le ministère de l'Intérieur souhaitait créer un système centralisé – dénommé SAFARI – utilisant le numéro d'identification établi par l'Institut National de la Statistique et des Études Économiques (INSEE) comme identifiant commun aux quelques quatre cents fichiers publics. Pour une présentation du contexte, v. A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 7, p. 17.
[623] C. Angeli et S. Mesnier, *Les micros du Canard,* Les arènes, 2014.
[624] V. *supra*, nº 1.
[625] Le film *La vie des autres* est une illustration des dangers de la surveillance, F. Henckel von Donnersmarck, *La vie des autres*, 2006.
[626] M. Leuenberger et J. Meier, « Évènements survenus au DFJP. Rapport de la commission d'enquête parlementaire », Parlement suisse, nº 89.006, 22 nov. 1989.
[627] Ce courant se concrétise par la publication d'un rapport annuel du Conseil d'État (Conseil d'État, « Les conséquences du développement de l'Informatique sur les libertés publiques et privées et sur les décisions administratives », *Rapport Public 1969-1970*, La Documentation française, 1970), par le dépôt ou l'adoption de plusieurs projets et propositions de lois, (v. not. la proposition de loi de Michel Poniatowski tendant à la création d'un comité de surveillance et d'un tribunal de l'informatique, Assemblée nationale, nº 1454, déposée le 25 nov. 1970).

personnelles, notamment aux États-Unis[628], en Allemagne[629], en Belgique[630], en Suède[631] et, quelques années plus tard, en Suisse[632].

Si le législateur français avait initialement commencé à protéger certaines catégories de données[633], le scandale SAFARI a définitivement scellé le sort de l'approche législative retenue[634] : la loi française relative aux traitements de données personnelles est une loi d'ensemble[635].

176. La loi du 6 janvier 1978. La loi 78-17 relative à l'informatique, aux fichiers et aux libertés, souvent dénommée « loi Informatique et libertés » fut adoptée le 6 janvier 1978. Cette loi est courte et d'application large : elle concerne les traitements automatisés et manuels d'informations nominatives effectués par le secteur public et privé[636]. Les débats législatifs ne laissent pas de place au doute : c'est bien pour

---

[628] Aux États-Unis, le rapport publié en 1973 a théorisé les principes cardinaux de la protection des données personnelles (les *Fair Information Privacy Principles*), v. *infra*, nº 304. Ce rapport a favorisé l'adoption du *Privacy Act* en 1974 qui règlemente les traitements d'informations personnelles par les agences fédérales, v. Pub. L. du 31 déc. 1974, nº 93-579, codifiée au 5 U.S.C. § 552a (2000). Pour une étude sur la jurisprudence et la loi, v. Department of Justice, *Overview of the Privacy Act of 1974*, 2015. Contrairement à ce qui est affirmé dans le manuel français *Informatique et libertés* (A. Debet, J. Massot et N. Métallinos, *Informatique et libertés : La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 6, p. 17), cette loi garantit plus qu'un simple « droit d'accès pour les citoyens ». En effet, après avoir rappelé la valeur fondamentale du droit à la *privacy*, cette loi énonce six principes pour garantir l'effectivité de sa protection : un droit de connaissance, un droit d'opposition sur l'utilisation ou la diffusion des informations, un droit d'accès et de modification, une obligation liée à la qualité et la sécurité des données, toute dérogation à ces principes ne peut être effectuée que par une loi motivée par l'intérêt général. Un droit de recours est également consacré dans cette loi.

[629] Le *land* allemand de Hesse a ouvert la voie en 1970 avec l'adoption d'une loi sur les données personnelles, v. « Loi du Land de Hesse (RFA) du 7 octobre 1970 », in : Gesetz-und Verordnungsblatt für das Land Hesse, Teil I Nr 41, Wiesbaden, 12X1970. Texte français in : G.B.F. Niblett, *L'information numérique et la protection des libertés individuelles*, OCDE, 1971, p. 51 s.

[630] Proposition de loi des sénateurs Person, Hambye et Vanderpoorten relative à la protection de la vie privée et de la personnalité, Chapitre IV, Du contrôle des informations traitées par des moyens électroniques ou autres, Sénat de Belgique, Session de 1971-9172, document nº 142.

[631] Loi SFS 1973-289 sur les données à caractère personnel, 11 mai 1973 et arrêté nº 1973-291.

[632] Une législation transversale en matière de protection des données a été adoptée au début des années 1990, v. F. Riklin, « La protection des données personnelles : aspects de droit pénal. Situation actuelle en Suisse », *RID comp.* 1987, vol. 39, nº 3, p. 677.

[633] V. not. loi nº 70-539 du 24 juin 1970 concernant la centralisation de la documentation relative à la circulation routière, *JORF* 25 juin 1970, p. 65, et la loi , loi nº 70-1318 du 31 déc. 1970 portant réforme hospitalière, *JORF* 3 janv. 1971, p. 65.

[634] En novembre 1974, le conseiller d'État Bernard Tricot était chargé d'établir un rapport sur la question « Informatique et libertés », v. B. Tricot, « Rapport de la commission Informatique et libertés », La Documentation française, 1975. Ce rapport fut largement entériné par le projet de loi Informatique et libertés étudié fin 1977 au Parlement, v. projet de loi de Jean Lecanuet relatif à l'informatique et aux libertés, Assemblée nationale, nº 2516, déposé le 9 août 1976. Signe de l'intérêt parlementaire pour cette thématique, d'autres travaux avaient accompagné ce projet, v. not. la proposition de loi de Pierre-Bernard Cousté tendant à créer une Commission de contrôle des moyens d'informatique afin d'assurer la protection de la vie privée et des libertés individuelles des citoyens, Assemblée nationale, nº 1004, déposée le 4 avril 1974 ; v. aussi la proposition de loi de Lucien Villa et plusieurs de ses collègues sur les libertés, les fichiers et l'informatique, Assemblée nationale, nº 3092, déposée le 21 juin 1977.

[635] Sur les effets d'une approche législative d'ensemble sur la notion de donnée à caractère personnel, v. *supra*, nº 136.

[636] Loi nº 78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* 7 janv. 1978, p. 227. Malgré un calendrier resserré, ce texte a fait l'objet d'intenses discussions et d'une navette qui s'est clôturée par le recours à la procédure de commission mixte paritaire, v. A. de Laubadère, « Chronique générale de législation, Loi relative à l'informatique, aux fichiers et aux libertés », *AJDA* 1978, p. 146, spéc. p. 147. Pour une présentation

répondre aux spécificités des atteintes à la vie privée permises par l'informatique que cette loi a été adoptée.

177. La loi Informatique et libertés, un moyen de garantir le droit au respect de la vie privée. À l'origine, le droit des données personnelles a été élaboré comme une déclinaison du droit au respect de la vie privée[637]. D'ailleurs, Jean Foyer avait proclamé qu'il convient « dans une matière aussi neuve, de se souvenir du proverbe : "Qui trop embrasse mal étreint". C'est pourquoi le projet prévoit que les dispositions légales *s'appliqueront seulement aux traitements automatisés d'informations nominatives*, les seules qui soient vraiment dangereuses pour la vie privée et pour les droits individuels des citoyens »[638]. L'article premier de la loi retranscrit cette intention en affirmant que « l'informatique doit être au service de chaque citoyen. (…) Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». Le plaidoyer ne peut être plus clair : la loi Informatique et libertés est un moyen juridique supplémentaire pour prévenir les atteintes aux droits individuels et à la vie privée[639]. L'encadrement des traitements d'informations nominatives vise donc à établir les garanties nécessaires à un développement de l'informatique respectueux de la vie privée.

B. Des fondements distincts

178. L'autonomie de fondements en France. En dépit de la consécration légale du droit au respect de la vie privée en 1970, le législateur français a privilégié, moins d'une décennie plus tard, l'adoption d'un fondement distinct pour encadrer les traitements d'informations personnelles. En droit français, ce sont donc deux fondements autonomes qui protègent les informations relatives aux personnes physiques.

---

complète du texte, v. H. Maisl, « La maîtrise d'une interdépendance. Commentaire de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés », *JCP G* 1978, I, p. 2891 ; P. Kayser et J. Frayssinet, « La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés », *RDP* 1979, p. 633.

637 V. *Rép. civ.* Dalloz, *V°* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), n° 8 ; Y. Détraigne et A.-M. Escoffier, « Rapport d'information relatif au respect de la vie privée à l'heure des mémoires numériques », Sénat, n° 441, 27 mai 2009, p. 15. Comp. A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, n° 497, p. 220 qui considèrent que cette protection vise « à protéger les personnes physiques de l'ensemble des conséquences préjudiciables au regard de leurs droits et libertés, dont la protection de la vie privée est seulement une composante ».

638 J. Foyer, 1re séance du mardi 4 oct. 1977, *JORF AN* 5 oct. 1977, n° 79, p. 5783.

639 Sur le caractère initialement préventif de la loi, v. *infra*, nos 304 s.

179. L'autonomie de fondements en droit de l'Union européenne. Dans un premier temps, le droit de l'Union européenne a protégé les libertés individuelles de manière prétorienne[640], se fondant sur les principes généraux du droit[641]. Dans un second temps, ces droits ont été consacrés dans des textes. Le droit au respect de la vie privée et le droit des données à caractère personnel occupent désormais une place éminente dans le droit de l'Union européenne. Ainsi, l'article 16 du traité sur le fonctionnement de l'Union européenne reconnaît expressément le droit de toute personne à la protection de ses données à caractère personnel[642], et la Charte des droits fondamentaux de l'Union européenne distingue le droit au respect de la vie privée garanti par son article 7 du droit à la protection des données à caractère personnel affirmé par son article 8[643]. En droit dérivé, les textes distinguent également entre la protection des « données à caractère personnel »[644] et celle de la « vie privée »[645].

Ainsi, le droit européen reconnaît également deux fondements juridiques distincts pour protéger les informations se rapportant à une personne physique.

180. L'influence de l'autonomie de fondements sur les notions. L'existence de deux fondements distincts, dont l'objet commun est de protéger des informations concernant les personnes, a favorisé une conception étendue de la notion de donnée à caractère personnel. En effet, quel serait l'intérêt de protéger strictement les mêmes informations sur deux fondements juridiques distincts ? Une telle dualité engendrerait

---

[640] Les traités communautaires ne contenaient pas de disposition relative aux droits de l'Homme, mais avaient plutôt pour objectif d'instaurer un marché commun. Tout au plus étaient mentionnés, dans le traité établissant une Communauté économique, la libre circulation des travailleurs (art. 48) et le principe de non-discrimination en raison de la nationalité (art.7) et cela, dans le seul objectif de favoriser la mise en place du marché commun, v. C. Gauthier, S. Platon et D. Szymczak, *Droit européen des droits de l'Homme,* Sirey, 2016, nº 55, p. 30.

[641] C. Lumaret, *L'effet horizontal de la Charte des droits fondamentaux de l'Union européenne*, th. Paris II, 2015, nº 2. V. part. l'arrêt *Stauder* dans lequel la Cour de justice avait eu à se prononcer sur l'évaluation des conséquences de la divulgation d'informations personnelles, CJCE, 12 nov. 1969, *Stauder* c. *Ville d'Ulm*, C-29/69, § 7.

[642] Le paragraphe premier de l'article 16 prévoit que « toute personne a droit à la protection des données à caractère personnel la concernant ». Cet article a considérablement étendu le droit initialement reconnu par l'article 286 du traité instituant la Communauté européenne.

[643] Charte des droits fondamentaux de l'Union européenne, *JOUE* 30 mars 2010, C-83/02, p. 389 s.

[644] V. not. règlement UE nº 2016/679 et la directive UE nº 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, *JOUE* 4 mai 2016, L-119/89, p. 89 s.

[645] V. not. directive CE nº 2002/58 du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *JOCE* 31 juill. 2002, L-201, p. 37 s.

beaucoup de confusion pour les personnes traitant ces informations puisqu'elles devraient respecter deux corps de règles différents[646].

Ainsi, l'adoption d'un fondement séparé pour protéger toutes les informations liées aux personnes, même celles indirectement identifiantes, a encouragé une émancipation de la notion de donnée à caractère personnel par rapport à celle de vie privée[647]. Les observations faites quant aux effets de la distinction entre les simples données à caractère personnel et les données sensibles[648] sont parfaitement transposables à la séparation entre la notion de vie privée et celle de donnée à caractère personnel. En effet, en protégeant largement les informations relatives à la vie privée, cela encourage une acception encore plus large de la notion de donnée à caractère personnel. L'essor de cette notion est également lié aux évolutions techniques.

§ II. Les évolutions techniques

181. Plan. L'informatique a profondément modifié les méthodes d'identification des personnes. Les traitements de données sont devenus si complexes et ingénieux qu'un nombre croissant de données se rapportent aux personnes physiques (A). L'exemple de la qualification juridique de l'adresse IP comme donnée à caractère personnel témoigne de l'adaptabilité de cette notion face aux évolutions technologiques (B).

A. Exposé : l'évolution des techniques d'identification

182. L'évolution des méthodes d'identification. Le plus ancien régime d'identification consistait en un face à face entre personnes dans lequel les aspects visuels et les relations personnelles prédominaient[649]. D'ailleurs, le terme « identité » vient du grec *idein*, signifiant vision[650]. À ce régime d'identification s'ajoutent, dès le Moyen-Âge, les sceaux, armoiries, signatures et insignes. Ces signes extérieurs

---

[646] Comp. obs. J. Carbonnier ss Cass. civ. 1re, 19 juill. 1960, *RTD civ.* 1961, p. 333, selon l'auteur « lorsque le droit positif met deux moyens juridiques à la disposition du même individu, le sens le plus élémentaire de ce double don est le cumul ».

[647] Cette affirmation doit toutefois être relativisée puisque, devant les juridictions, des liens entre les notions persistent, v. *infra*, nos 206 s.

[648] V. *supra*, nos 141 s.

[649] « Dans les sociétés dites "traditionnelles", sans écriture, fondées sur l'oralité et l'interconnaissance, l'identification des individus repose sur les relations de face à face et la mémoire du groupe local et familial », I. About et V. Denis, *Histoire de l'identification des personnes*, La Découverte, 2010, p. 4 et 103. Sur l'identification, v. aussi, G. Noiriel, *L'identification. Genèse d'un travail d'État*, Belin, 2007 ; V. Denis, « Petite histoire des documents d'identité : la France des Lumières », *Documentaliste-Sciences de l'Information* 2010, vol. 47, p. 32.

[650] J. Markale, « Le nom, la parole et la magie », in *Corps Écrit* 1983, no 8, p. 38.

d'identité apparaissent comme des substituts de la personne, permettant de l'identifier indirectement[651]. À partir du XV^e^ siècle, l'identification est marquée par le développement spectaculaire des identités de papier : l'enregistrement du nom devient la norme[652]. La prise en compte, à la fin du XIX^e^ siècle, des données corporelles telles que les empreintes digitales, la taille ou l'image des personnes, amplifie encore le nombre d'éléments participant à leur identification[653]. Dans nos sociétés connectées, l'amplification du nombre de données générées a encore accru le nombre d'éléments contribuant à l'identification indirecte des personnes.

183. Une augmentation du nombre de données. L'utilisation constante de l'informatique et du numérique engendre une augmentation du volume de données générées. Les chiffres sont considérables : selon Monsieur Dominique Cardon « si l'on numérisait toutes les communications et les écrits depuis l'aube de l'humanité jusqu'en 2003, il faudrait cinq milliards de gigabits pour les mettre en mémoire. Aujourd'hui, nous générons ce volume d'informations numériques en deux jours »[654]. La société dans laquelle nous vivons est donc, sans conteste, une société de données[655].

184. Des méthodes ingénieuses pour identifier les personnes. Pour Monsieur Paul Ohm, les techniques d'identification tracent deux courbes qui progressent inlassablement vers le haut : la puissance des outils et la richesse des informations extérieures[656]. Ces courbes contribuent à rendre l'identification plus facile. Il est vrai que la liste des éléments pertinents qui concourent à la révélation d'une identité est longue et ne cesse de se diversifier[657]. Grâce au développement de la puissance de calcul des ordinateurs et à d'ingénieux croisements, les petites traces disséminées par les personnes, d'apparence anodines, sont utilisées pour révéler des informations sur elles[658]. Ainsi, un nombre toujours plus important d'informations contribue au

---

[651] I. About et V. Denis, *Histoire de l'identification des personnes*, La Découverte, 2010, p. 11.
[652] I. About et V. Denis, *Histoire de l'identification des personnes*, La Découverte, 2010, p. 33 s. L'apparition du passeport à la fin du XVIII^e^ siècle vise à échapper à la domination des apparences : « il s'agit de trouver des indices objectifs, fiables et relativement stables sur l'identité des voyageurs », v. G. Dubey, « Nouvelles techniques d'identification, nouveaux pouvoirs. Le cas de la biométrie », *Cahiers internationaux de sociologie* 2008, n° 125, p. 263, spéc. p. 267.
[653] I. About et V. Denis, *Histoire de l'identification des personnes*, La Découverte, 2010, p. 71.
[654] D. Cardon, *À quoi rêvent les algorithmes : nos vies à l'heure des big data,* Seuil, 2015, p. 11.
[655] V. *supra*, n° 2.
[656] P. Ohm, « Broken promises of privacy : responding to the surprising failure of anonymization », *UCLA Law Review* 2010, vol. 57, p. 1701 s. [57 UCLA L. REV. 1701], spéc. p. 1731.
[657] F. Lesaulnier, *L'information nominative,* th. Paris II, 2005, n^os^ 27 s., p. 44 s.
[658] Pour une étude concernant le risque de réidentification des données et les dispositifs de villes intelligentes, v. P. Mouron, « La protection des données personnelles dans l'environnement urbain. De la mesure d'audience

rattachement avec une personne : cartes, images, puces, plaques, traces, numéros, empreintes, sont quelques exemples d'informations participant aujourd'hui à l'identification d'une personne[659]. Les méthodes actuelles d'identification sont donc en profonde rupture avec les méthodes originelles de l'identification : ce n'est plus une personne qui en identifie une autre (par la vision), mais des logiciels qui traitent des informations de toute nature pour établir un lien avec la personne.

185. La difficulté d'effacer le lien entre une donnée et une personne. À cette augmentation des données contribuant à l'identification s'ajoute la difficulté d'effacer le lien entre une donnée et une personne. En effet, lorsqu'un tel rattachement a existé, une disjonction définitive est très difficile[660]. Plusieurs exemples témoignent de cette difficulté, notamment due à la transformation des méthodes d'identification et à l'ingéniosité des *data-scientists*[661].

L'un des exemples les plus illustratifs[662] est celui de la mise à disposition en 2013 par la Commission des Taxis et des Limousines de New York d'une base de données des trajets en taxi[663]. Avant sa publication, la base de données des quelques cent-soixante-treize millions de trajets avait été expurgée des éléments d'identification pour permettre son exploitation tout en préservant la confidentialité des déplacements[664]. En apparence, peu de choses rattachent un déplacement de taxi à une personne spécifique. Pourtant, l'ingénieur Vijay Pandurangan avait rapidement réussi à rattacher les conducteurs de taxi aux différents trajets[665]. Quelques semaines plus

publicitaire aux villes intelligentes », *RLDI* 2017, nº 139, p. 54, spéc. p. 58. Pour un aperçu de ces risques dans le domaine de la santé, v. C. Castets-Renard, « Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé : big data et open data », *RLDI* 2014, nº 108, p. 38, spéc. p. 44.

[659] Pour un exposé sur la montée en puissance des traces laissées par les utilisateurs de l'informatique, v. E. Netter, *Numérique et grandes notions du droit privé. La personne, la propriété, le contrat*, mémoire en vue de l'habilitation à diriger des recherches en droit privé, Picardie, 20 nov. 2017, nos 49 s., p. 69 s.

[660] Sur cette question, v. G29, WP 216, Avis 5/2014 sur les techniques d'anonymisation, 10 avr. 2014, p. 9 s. G. Gorce et F. Pillet, « Rapport d'information sur l'open data et la protection de la vie privée », Sénat, nº 469, 16 avr. 2014, p. 46. Pour une analyse de l'effet du *big data* sur les notions fondamentales, v. A. Bensamoun et C. Zolynski, « *Big data* et *privacy* : comment concilier nouveaux modèles d'affaires et droits des utilisateurs ? », colloque du Forum des sciences sociales, Montréal, 15 oct. 2013, *LPA* 18 août 2014, nº 164, p. 8, § 11 s.

[661] Le *data-scientist* est le « spécialiste de l'extraction et de l'exploitation d'informations pertinentes à partir de mégadonnées, qu'il organise, traite et interprète à l'aide d'outils statistiques, mathématiques et informatiques », v. Commission d'enrichissement de la langue française, « Vocabulaire de l'informatique et de l'internet (liste de termes, expressions et définitions adoptées) », *JORF* 26 sept. 2017, nº 0225, texte 110.

[662] D'autres exemples illustrent ces méthodes, v. not. G. Gorce et F. Pillet, « Rapport d'information sur l'open data et la protection de la vie privée », Sénat, nº 469, 16 avr. 2014, p. 46.

[663] J. K. Trotter, « Public NYC taxicab database lets you see how celebrities tip », *Gawker* 23 oct. 2014.

[664] Sur la différence entre l'anonymisation et la pseudonymisation, v. *supra*, nos 119 s.

[665] V. Pandurangan, « On taxis and rainbow. Lessons from NYC's improperly anonymized taxi logs », *Medium* 21 juin 2014. Cette possibilité de réidentification était liée à une faible fonction de hachage utilisée pour retirer les éléments identifiants de la base de données. Le hachage est une « opération consistant à déterminer une information de taille fixe et réduite à partir d'une donnée de taille indifférente, de telle façon que deux données quelconques aient une faible probabilité de produire le même résultat », v. Commission d'enrichissement de la

tard, l'étudiant Anthony Tockar utilisait des photographies diffusées en ligne de personnalités publiques entrant ou sortant de taxis dont le numéro était visible et montrait qu'il était également possible de réidentifier certains passagers[666]. Grâce à cette technique, il avait réussi à identifier, au sein de la base de données, les lieux de prise en charge et de dépose, le tarif de la course et le pourboire laissé par ces passagers.

D'autres exemples confortent ces analyses. Des chercheurs ont ainsi montré que les données agrégées du pourcentage de la batterie d'un téléphone permettent de révéler sa localisation[667]. La façon dont un joueur tient sa manette serait également une donnée indirectement identifiante[668]. Les exemples sont nombreux et ne cessent d'augmenter, ce qui engage à se demander s'il existe encore des données non personnelles[669]. Les questions ayant entouré la qualification juridique de l'adresse IP illustrent bien ce mouvement d'expansion de la notion.

B. Exemple : l'adresse IP

186. Définition et qualification de l'adresse IP. Par nature, une adresse IP est représentée par une suite de chiffres permettant d'identifier une machine lorsqu'elle se connecte à Internet[670]. Ainsi, à première vue, rien n'encourage à qualifier une adresse IP comme une donnée à caractère personnel. Pourtant derrière l'adresse IP se trouve parfois une personne physique : l'adresse IP est alors le masque qu'elle prend pour naviguer sur Internet. De vifs débats doctrinaux ont contesté la nature juridique de ces adresses[671]. Tranchés par les juridictions en faveur de la reconnaissance comme donnée

---

langue française, « Vocabulaire de l'informatique et de l'internet (liste de termes, expressions et définitions adoptées) », *JORF* 27 févr. 2003, nº 0049, p. 3531, texte 77.

666 A. Tockar, « Riding with the stars : passenger privacy in the NYC taxicab dataset », *Neustar Research* 15 sept. 2014.

667 Y. Michalevsky, A. Schulman, G. Arumugam, D. Boneh et G. Nakibly, « Power spy : location tracking using mobile device power analysis », *Security Symposium* 2015.

668 Les constructeurs de manettes de jeux vidéo font des analyses sur la manière dont leurs joueurs les tiennent afin de les identifier, v. Patent Application Publication, Anderson *et al.* (Sony), 20 août 2020, pub. nº US 2020/0261803, p. 5.

669 R. Perray et J. Uzan-Naulin, « Existe-t-il encore des données non personnelles ? », *Dalloz IP/IT* 2017, p. 286 ; H. Guillard, « Critique du Web2 (3/4) : Toutes les données sont devenues personnelles », *Internetactu.net* 21 sept. 2009. V. aussi A. Bensamoun et C. Zolynski, « *Cloud computing* et *big data*. Quel encadrement pour ces nouveaux usages des données personnelles ? », *Réseaux* 2015, nº 189, p. 103. Pour Mesdames Valérie-Laure Benabou et Judith Rochfeld, « aujourd'hui, tout est devenu donnée personnelle », V.-L. Benabou et J. Rochfeld, *À qui profite le clic ? Le partage de la valeur à l'ère numérique*, Odile Jacob, 2015, p. 58.

670 J.-G. Grenier, *Dictionnaire d'informatique et d'Internet. Anglais-Français,* La maison du dictionnaire, 2000, *Vº* « Internet protocol address ». Sur une description de la nature technique et juridique de l'adresse IP v. C. Guerrier, « Les aspects techniques de la régulation des données personnelles : la question du numéro IP », *Légicom* 2009, nº 42, p. 127 s.

671 V. parmi les nombreux commentaires sur le sujet, M. Bénéjat, « Les droits sur les données personnelles », in *Droits de la personnalité,* dir. J.-C. Saint-Pau, LexisNexis, 2013, nº 934, p. 567 s. ; C. Caron, « Qualification de l'adresse "IP" : état des lieux jurisprudentiel », *CCE* 2007, nº 12, comm. 144 ; F. Mattatia, « L'adresse IP est-elle une donnée à caractère personnel ? », *Gaz. Pal.* 2008, nº 15, p. 9 ; M. Teller, « Les difficultés de l'identité

à caractère personnel[672], ces débats incarnent surtout la difficulté pour les acteurs de ce droit à limiter l'application de la notion de donnée à caractère personnel.

187. Établir un lien entre une adresse IP et une personne. Lorsque l'adresse IP est le fruit d'une connexion instiguée par une personne, elle peut contribuer à obtenir de nombreuses informations sur celle-ci. Toutefois, comme pour la plupart des données indirectement identifiantes, le rattachement entre l'adresse IP et la personne ne peut être établi que par son croisement avec d'autres données.

C'est pourquoi le G29 et la CJUE ont considéré que l'adresse IP est, pour le fournisseur de services de médias en ligne, une donnée à caractère personnel lorsqu'il « dispose de moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à Internet de cette personne »[673]. En effet, pour établir un lien entre l'adresse IP et la personne physique, deux actions sont souvent nécessaires. D'abord, il faut obtenir du fournisseur d'accès à Internet l'identification du titulaire du forfait associé à l'adresse IP. Ensuite, il faut replacer cette information dans un contexte, c'est-à-dire la croiser avec d'autres éléments, souvent d'autres données personnelles, afin de rétablir un lien entre cette adresse IP et la personne[674].

Pour autant, cette identification en deux temps n'est pas la seule technique aboutissant au rattachement entre une adresse IP et une personne. Ainsi, lorsqu'un utilisateur de site Internet révèle son identité lors d'une session, le croisement de l'adresse IP avec la date de cette session permet d'effectuer ce lien[675]. Par ailleurs, certains responsables du traitement collectent d'autres informations dans le but de les croiser et d'identifier l'utilisateur. Par exemple, il est fréquent pour les responsables du traitement de localiser l'adresse IP grâce aux techniques de « GeoIP »[676] pour

---

numérique : quelle qualification juridique pour l'adresse IP ? », *D.* 2009, p. 1988 ; G. Peronne et E. Daoud, « L'adresse IP est bien une donnée à caractère personnel », *Dalloz IP/IT* 2017, p. 120.

[672] En France, v. Cass. civ. 1re, 3 nov. 2016, nº 15-22.595, *Bull. civ.* 2016, nº 206, p. 251. En Europe, v. not. CJUE, 19 oct. 2016, *Patrick Breyer* c. *Bundesrepublik Deutschland*, C-582/14, § 49.

[673] CJUE, 19 oct. 2016, *Patrick Breyer* c. *Bundesrepublik Deutschland*, C-582/14, § 49. G29, WP 37, Document de travail. Le respect de la vie privée sur Internet. Une approche européenne intégrée sur la protection des données en ligne, 21 nov. 2000, p. 9. V. déjà CJUE, 24 nov. 2011, *Scarlet Extended SA* c. *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, § 51. Une interprétation *a contrario* laisse penser que cette adresse pourrait donc ne pas recevoir le qualificatif de donnée à caractère personnel, la portée de cette solution n'est donc peut-être pas aussi large que certains commentateurs ont pu l'affirmer, v. not. G. Péronne et E. Daoud, « L'adresse IP est bien une donnée à caractère personnel », *Dalloz IP/IT* 2017, p. 120.

[674] Dans sa thèse, Madame Frédérique Lesaulnier parle de « faisceaux » de données pour identifier la personne, v. F. Lesaulnier, *L'information nominative,* th. Paris II, 2005, nº 45, p. 64.

[675] En effet, l'opérateur du site peut faire un tel croisement, CJUE, 19 oct. 2016, *Patrick Breyer* c. *Bundesrepublik Deutschland*, C-582/14, § 20.

[676] UserInsights, « How the geolocation works ».

déterminer la position géographique de l'adresse IP. Ainsi, l'adresse IP est souvent un indice s'inscrivant dans un faisceau plus large d'informations concourant, ensemble, à la supposition de l'identité de la personne.

188. Caractère incertain de l'identification. En tout état de cause, la plupart du temps, le lien effectué entre l'adresse IP et la personne a rarement un caractère certain. Par exemple, une adresse IP publique est souvent partagée entre plusieurs utilisateurs au sein d'un foyer ou d'une entreprise, rendant l'identification de l'utilisateur parmi les différents membres de ce lieu plus incertaine[677]. Il se peut aussi qu'une tierce personne s'attribue une adresse IP particulière[678], ou qu'un utilisateur navigue *via* un réseau privé virtuel (VPN)[679]. Il arrive également que le fournisseur d'accès à Internet soit obligé de donner, au même moment, la même adresse IP à plusieurs foyers[680]. Ces exemples illustrent l'incertitude relative au rattachement existant entre une adresse IP et une personne physique.

Cette incertitude est encore plus grande lorsque l'adresse IP est dynamique[681]. Ces adresses IP sont de nature instable puisqu'elles sont attribuées à chaque connexion

[677] En réseau informatique, certains routeurs font de la traduction d'adresses (NAT, *Network Address Translation*), c'est-à-dire qu'ils font correspondre des adresses IP privées à une adresse IP publique. En effet, l'opérateur fournit une adresse IP publique au routeur et celui-ci numérote ses équipements en utilisant un adressage privé. Lorsqu'un paquet portant une adresse source privée veut sortir vers Internet, le routeur y insère une adresse publique (visible depuis l'extérieur). Le routeur mémorise alors la correspondance entre l'adresse IP publique et l'IP privée, et lorsqu'un paquet revient vers lui, il fait l'opération inverse en remplaçant l'adresse destination publique par l'adresse privée d'origine, v. J. Akoka et I. Comyn-Wattiau (dir.), *Encyclopédie de l'informatique et des systèmes d'information*, Vuibert, 2006, p. 54.

[678] Le tribunal de commerce de Cannes a ainsi considéré qu'une adresse IP, même utilisée régulièrement par un client, ne suffit pas à établir la preuve d'un virement effectué au départ du compte bancaire dudit client. Pour le tribunal, « si des faussaires ont pu se procurer toutes les données leur permettant d'usurper l'identité des époux X., il est logique d'imaginer qu'ils ont également pu connaître l'adresse IP de l'ordinateur qu'ils utilisaient pour consulter leur compte bancaire », Trib. com. Cannes, 27 juill. 2017, nº 2015F00305, sur ce jugement, v. J. Lasserre Capdeville, « La présence d'une adresse IP n'est pas une preuve suffisante en matière de virement », *Dalloz IP/IT* 2017, p. 661. Cette interprétation a été confirmée en tout point par la cour d'appel d'Aix-en-Provence, v. CA Aix-en-Provence, 3e et 4e ch., 21 févr. 2019, nº 17/15864.

[679] Un réseau virtuel privé (en anglais *Virtual Private Network,* VPN) est un système permettant de créer un lien direct entre deux ordinateurs distants, comme s'ils étaient sur le même réseau local. Souvent chiffré, il permet aussi généralement de bénéficier d'une passerelle pour utiliser l'accès à Internet de l'ordinateur distant, ce qui permet de bénéficier d'une autre adresse IP et, éventuellement, de masquer son origine géographique, v. A. Piraina, « À quoi sert un VPN ? », *Numerama* 29 déc. 2019.

[680] Comme le notait le G29 dans son avis de 2000, le « nombre d'adresses IP est actuellement limité, et dépend de la longueur du champ de l'adresse IP dans le protocole. La version mise à niveau (IPversion6) du système d'adressage IP est en cours de développement sur la base de nombres de 128 bits », v. G29, WP 37, Document de travail. Le respect de la vie privée sur Internet. Une approche européenne intégrée sur la protection des données en ligne, 21 nov. 2000, p. 9. Sur l'attribution d'une même adresse IP à plusieurs foyers, v. G. Champeau, « Free peut attribuer la même adresse IP à plusieurs abonnés », *Numerama* 15 févr. 2016.

[681] Deux types d'adresses IP existent : lorsqu'elle est statique, elle est identique dans le temps ; lorsqu'elle est dynamique, elle est attribuée pour une seule session ou pour une durée définie.

ou changées selon une certaine périodicité, et les risques d'erreurs d'identification sont donc encore plus élevés[682].

En dépit du caractère incertain de l'identification permise par les adresses IP, les juridictions ont affirmé qu'elles relèvent de la notion de données à caractère personnel.

189. Les adresses IP sont des données à caractère personnel. La CJUE considère depuis plusieurs années que les adresses IP sont « des données protégées à caractère personnel, car elles permettent l'identification précise desdits utilisateurs »[683]. Plus récemment, la CJUE a étendu cette qualification aux adresses IP dynamiques[684]. Après une période d'incertitude sur la qualification de l'adresse IP, la Cour de cassation a finalement rejoint cette interprétation[685]. Pour la Haute juridiction, « les adresses IP, qui permettent d'identifier indirectement une personne physique, sont des données à

---

[682] Cela suppose en effet de connaître l'heure précise de connexion, aux fins d'identification de l'internaute titulaire de l'adresse IP litigieuse au moment des faits

[683] CJUE, 24 nov. 2011, *Scarlet Extended SA* c. *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, § 51. Comme le remarquait très justement l'avocat général Monsieur Pedro Cruz Villalón, « la Cour n'a eu, jusqu'à présent, à connaître que de cas dans lesquels des données nominatives liées aux adresses IP étaient en cause. Elle n'a, en revanche, jamais encore eu l'occasion d'examiner si une adresse IP pouvait être considérée, en tant que telle, comme une donnée personnelle », v. conclusions de l'avocat général Pedro Cruz Villalón, présentées le 14 avr. 2011, dans l'affaire C-70/10, *Scarlet Extended SA* c. *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, § 44. La Cour de justice a récemment considéré que « les adresses IP pouvant être utilisées pour effectuer notamment le traçage exhaustif du parcours de navigation d'un internaute et, par suite, de son activité en ligne », elles « permettent d'établir le profil détaillé de ce dernier », CJUE, 6 oct. 2020, *La Quadrature du Net* c. *Premier ministre*, C-511/18, C-512/18 et C-520/18, § 153.

[684] CJUE, 19 oct. 2016, *Patrick Breyer* c. *Bundesrepublik Deutschland*, C-582/14, § 49. La CJUE a toutefois restreint la qualification de donnée à caractère personnel aux seules adresses IP pour lesquelles il existe, pour la personne traitant l'adresse, des *moyens légaux* permettant de faire identifier la personne concernée. En pratique, comme la plupart des pays européens ont, dans leur droit national, un tel mécanisme (il s'agit des règles relatives à la conservation des données), cette condition ne restreint que très relativement la qualification de ces adresses en données à caractère personnel. Ces règles sont toutefois susceptibles d'évoluer dès lors que la Cour de justice a considéré, à nouveau, que l'obligation, à titre préventif, de conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation était contraire au droit européen, v. CJUE, 6 oct. 2020, *La Quadrature du Net* c. *Premier ministre*, C-511/18, C-512/18 et C-520/18, § 168. V. déjà, CJUE, 8 avril 2014, *Digital Rights Ireland Ltd* c. *Minister for communications et al. et Kärntner Landersregierung*, C-293/12 et C-594/12 et CJUE, 21 déc. 2016, *Tele2 Sverige AB* c. *Post-och telestyrelsen,* C-203/15 et C-698/15.

[685] La cour d'appel de Paris avait rejeté la qualification de donnée à caractère personnel pour les adresses IP dans le contexte d'actes de contrefaçon en ligne, v. CA Paris, 13e ch., 27 avril 2007, nº 06/02334 ; CA Paris, 13e ch., 15 mai 2007, nº 06/01954, sur cette décision, v. C. Caron, « Qualification de l'adresse "IP" : état des lieux jurisprudentiel », *CCE* 2007, nº 12, comm. 144. La Cour de cassation, dans un arrêt du 13 janvier 2009, avait également retenu que le fait, parmi d'autres actions, de relever une adresse IP pour pouvoir localiser par le biais du fournisseur d'accès à Internet l'auteur des contrefaçons ne constituait pas un traitement de données à caractère personnel, v. Cass. crim., 13 janv. 2009, nº 08-84.088, *Bull. crim.* 2009, nº 13. La doctrine était divisée sur l'interprétation de cet arrêt. Une partie des auteurs considérait qu'il entérinait la solution de la cour d'appel de Paris, v. not. C. Caron, « Validité des constats effectués par des agents assermentés », *CCE* 2009, nº 4, comm. 31. Une autre partie des auteurs considérait à l'inverse que la Cour de cassation avait évité de répondre à la question de droit, v. not. L. Flament, « Les constatations visuelles effectuées sur Internet, sans recourir à un traitement préalable de surveillance automatisée, ne constituent pas un traitement de données à caractère personnel », *Dr. pén.* 2009, nº 5, étude 10. À l'opposé, la cour d'appel de Rennes avait tendance à accueillir favorablement cette qualification pour les adresses IP (v. CA Rennes, 23 juin 2008, nº 07/0121) avant de se raviser (v. CA Rennes, 28 avril 20015, nº 14/05708). Sur les évolutions de la jurisprudence sur ce sujet et le refus de prise de position par le Gouvernement en 2015, v. Question écrite de Monsieur Édouard Courtial, nº 21517, *JORF* 19 mars 2013, p. 3019 et la réponse du Ministère de l'économie, industrie et numérique, *JORF* 10 nov. 2015, p. 8206.

caractère personnel »[686]. Une lecture grammaticale de cet attendu laisse penser que la Cour de cassation considère que toutes les adresses IP sont des données indirectement identifiantes. Pourtant, dans de nombreuses situations, elles ne sont pas liées, ni directement ni indirectement, à une personne physique[687]. Une seconde lecture de cet attendu, plus conforme à la nature technique de ces adresses, pourrait être que seules celles permettant l'identification indirecte d'une personne physique doivent être qualifiées de données à caractère personnel[688]. Cette lecture rend cette solution plus en phase avec la réalité technique de ces données[689]. En tout état de cause, il est désormais établi que les adresses IP sont considérées comme des données à caractère personnel.

190. L'extension de la notion en dépit des incertitudes quant à l'identification. Les vastes capacités de traitement et de recoupements de données indirectement identifiantes développées par certains responsables du traitement ont tendance à favoriser une interprétation extensive de la notion de donnée à caractère personnel[690]. Même si tous les responsables du traitement ne souhaitent pas opérer un rattachement entre la donnée indirectement identifiante et la personne, qu'ils n'en sont pas techniquement capables ou que le lien présente d'importants risques d'erreur, la donnée recevra tout de même la qualification de donnée à caractère personnel. En cas de doute sur la nature des données traitées, les responsables du traitement sont donc invités à considérer que les données relèvent de la notion de donnée à caractère personnel. Ainsi, plusieurs facteurs, tels que les avancées technologiques en matière de traitement de l'information et l'augmentation des données générées, participent assurément à l'expansion de la notion de donnée à caractère personnel. Même lorsque l'identification de la personne est incertaine, ou qu'elle n'est pas l'objectif du responsable du traitement, la donnée doit quand même être considérée comme relevant de la notion de donnée à caractère personnel.

---

[686] Cass. civ. 1re, 3 nov. 2016, no 15-22.595, *Bull. civ.* 2016, no 206, p. 251.
[687] C'est le cas notamment lorsque les adresses IP sont le numéro d'un simple serveur.
[688] Pour cela il aurait suffi de retirer la virgule présente dans l'attendu. Cette solution reléguerait cette qualification au pouvoir souverain des juges du fond.
[689] D'ailleurs, dans une ordonnance de référé du 2 août 2019, le tribunal de grande instance de Paris semble retenir une telle interprétation en considérant que les adresses IP « sont *susceptibles* de permettre d'identifier indirectement une personne physique et doivent dès lors être considérées comme des données à caractère personnel », TGI Paris, réf., 2 août 2019, no 19/53.997. En utilisant l'adjectif « susceptible », le juge civil met en exergue le fait que les adresses IP ne sont pas toujours en rapport avec une personne physique.
[690] L'adverbe « raisonnablement » cantonne seulement en apparence la notion, v. *supra,* no 123.

§ III. Les difficultés d'application du droit des données à caractère personnel

191. Des manquements récurrents. Parmi les nombreuses causes ayant favorisé l'expansion de la notion de donnée à caractère personnel figure sans nul doute la légèreté avec laquelle les règles ont été appliquées[691]. Les manquements au droit des données à caractère personnel sont longtemps restés sans conséquence pour leurs auteurs. Ainsi, de nombreux traitements de données à caractère personnel ont été mis en œuvre en dehors du cadre légal contraignant[692]. Ces traitements non conformes ont engendré, pour les personnes concernées notamment, un sentiment d'inadéquation du droit des données personnelles par rapport aux usages numériques, les encourageant à revendiquer une meilleure protection de leurs données.

192. Les effets de ces manquements. L'une des réponses des acteurs de la protection des données pour répondre aux défauts du droit des données à caractère personnel a été d'étendre la notion de donnée à caractère personnel, donnant ainsi l'illusion d'une meilleure protection des personnes. Les lacunes dans la mise en œuvre des dispositions de la loi Informatique et libertés ont donc contribué, au moins indirectement, à l'expansion de la notion de donnée à caractère personnel.

193. Conclusion de chapitre. Depuis l'adoption des premières règles relatives à la protection des informations nominatives, la notion de donnée à caractère personnel est appliquée de plus en plus largement. Initialement limitée aux informations dont le lien avec les personnes était quasiment intrinsèque à la donnée, la notion s'est développée pour inclure tous types d'informations. Pour encourager une acception large de la notion, le législateur a modifié ses termes, élargi sa définition et enrichi sa liste d'exemples. Les autorités de contrôle et les juridictions ont saisi cette opportunité pour

---

[691] Pour justifier ces violations, les entreprises invoquent souvent des dispositions trop contraignantes ou le besoin de délais supplémentaires pour se mettre en conformité. Par exemple, lors de l'examen du texte de réception en droit français du règlement européen, la rapporteur au Sénat avait été la porte-voix des petites et moyennes entreprises et avait demandé à ce qu'elles puissent obtenir des délais supplémentaires pour se mettre en conformité avec les obligations prévues par le texte européen, v. S. Joissains, « Rapport sur le projet de loi adopté par l'Assemblée nationale après engagement de la procédure accélérée relatif à la protection des données personnelles », Sénat, nº 350, 14 mars 2018, p. 9 et p. 212.

[692] V. par ex., sur les manquements aux obligations déclaratives, *infra*, nº 311. La CNIL a elle-même reconnu cette inefficacité puisqu'elle a considéré que « l'entrée en application du RGPD a marqué une forte prise de conscience des enjeux de protection des données, en France comme en Europe ». Selon l'institution, il s'agirait même d'une prise de conscience inédite, CNIL, « 1 an de RGPD : une prise de conscience inédite », 23 mai 2019.

interpréter de plus en plus largement la notion, afin de couvrir toutes les situations dans lesquelles une information peut se rattacher, même éventuellement, à une personne physique. Cette expansion s'explique notamment par les évolutions technologiques qui ont permis des recoupements inédits dévoilant ainsi l'identité ou la présence des personnes.

194. Conclusion de titre. Les législateurs européen et français ont choisi des termes particulièrement larges pour composer la notion de donnée à caractère personnel. De la notion de donnée, dont les contours sont immenses, à la notion de personne physique, laquelle s'étend au-delà de la conception civiliste classique, ces termes favorisent une interprétation large. En consacrant le principe d'un rattachement indirect entre la personne et la donnée, la notion prospère largement. L'avantage de ces termes est qu'ils lui permettent de s'adapter aux évolutions technologiques et ainsi d'éviter son obsolescence. Mais puisque de plus en plus de données renseignent aujourd'hui sur les personnes, la notion accueille un nombre toujours plus grand d'informations. Le lien entre la personne et la donnée n'a plus besoin d'être certain : il peut être éventuel, probable, voire réalisable uniquement par une faible minorité de responsables du traitement[693]. Ce mouvement trouve ses racines dans les premières interprétations de la notion d'information nominative effectuées par la CNIL. Rapidement, les juridictions ont rejoint cette tendance et ont, elles aussi, qualifié de plus en plus de données comme des données à caractère personnel. Aujourd'hui, ce mouvement a pris une telle ampleur que les limites entourant la notion de donnée à caractère personnel sont difficiles à tracer. Le développement des capacités de réidentification cumulé à l'augmentation de la production de données explique partiellement ce mouvement d'expansion. D'autres facteurs, tels que la distinction faite par le droit entre les données sensibles, les données relatives à la vie privée et les données à caractère personnel, encouragent également à retenir une conception étendue de la notion de donnée à caractère personnel. Pour autant, il semble que cette expansion ne soit pas sans risque pour la protection des personnes. Comme le remarquait déjà Jean Carbonnier, « à défaut de tout embrasser, ce qui serait embrasser trop »[694], il faut choisir ce qui doit recevoir une protection

[693] L'on pense aux responsables du traitement ayant les plus grandes capacités de traitement de l'information et dont les bases de données sur les personnes sont déjà conséquentes.
[694] J. Carbonnier, « En l'année 1817 », *Mélanges P. Raynaud*, Dalloz, 1985, p. 81 s., spéc. p. 81.

juridique. Pour éviter que la notion de donnée à caractère personnel n'embrasse trop, elle doit trouver des limites. Dans cet objectif, un cantonnement doit être proposé.

TITRE II – UNE NOTION À CANTONNER

195. L'objectif de la loi Informatique et libertés : la protection des personnes et de leurs libertés. L'emblématique article premier de la loi de 1978 affirmait 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 »[695]. Cette maxime renseigne sur le but de la loi : il s'agit d'établir les garanties nécessaires pour préserver les libertés et contribuer au respect de la vie privée face aux développements de l'informatique[696].

196. Les effets de l'expansion de la notion. Après plus de quatre décennies d'application, il est désormais évident que la notion de donnée à caractère personnel s'est étendue puisqu'elle inclut dans son giron toutes les informations liées aux personnes. Ce développement s'est fait de manière si naturelle que peu d'auteurs se sont intéressés à ses effets[697]. Pour autant, il convient tout de même de vérifier que cette expansion sert l'objectif du droit des données à caractère personnel, c'est-à-dire la protection des personnes.

197. Des propositions d'encadrement de la notion. En réalité, cette expansion ne sert pas toujours la protection des personnes et qu'elle a parfois tendance à avoir des effets contreproductifs. Dès lors, il conviendra de proposer un critère d'encadrement de la notion afin de savoir que celle-ci protège réellement les données relatives aux personnes.

---

[695] Sur l'importance de cet article, v. J. Frayssinet, « L'utilité et les fonctions d'une formulation d'objectifs : l'exemple de la loi du 6 janvier 1978 », *Revue de la recherche juridique* 1984, n° 4, p. 903 s. Sur l'objectif général de la loi, v. D. Gutmann, *Le sentiment d'identité. Étude de droit des personnes et de la famille*, th. Paris II, 2000, LGDJ, n° 289, p. 250 s.

[696] D'ailleurs, cette volonté n'est pas propre à la loi française puisque l'article 1er de la Convention 108 garantit à toute personne « le respect de ses droits et libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant ».

[697] La thèse de Madame Éloïse Gratton offre une analyse intéressante des effets de la conception large de l'information personnelle, v. É. Gratton, *Redefining personal information in the context of the Internet*, th. Paris II et Montréal, 2012, p. 71 s.

198. Plan. L'expansion de la notion de donnée à caractère personnel a des effets sur certaines libertés, notamment les libertés en lien avec l'information (Chapitre I). Pour encadrer cette expansion et s'assurer que la notion de donnée à caractère personnel ne restreint pas inopportunément la circulation de données, il conviendra de s'intéresser aux propositions d'encadrement (Chapitre II).

Chapitre I – Les effets de l'expansion de la notion de donnée à caractère personnel sur les libertés

199. Une étude limitée à certaines libertés. Le champ des libertés visées par l'article premier de la loi Informatique et libertés est immense. Il s'agit non seulement de l'identité humaine, des droits de l'homme, mais aussi de la vie privée et des libertés individuelles et publiques[698]. Pour autant, il apparaît que les développements de la notion de donnée à caractère personnel ne touchent pas toutes les libertés de manière égale. Ainsi, notre étude se limitera à l'étude des libertés les plus affectées par l'expansion de la notion.

200. Les effets de l'expansion sur la protection de la vie privée. L'un des principaux objectifs de la loi Informatique et libertés était de garantir, à l'ère de l'informatique, le droit au respect de la vie privée[699]. En principe, l'expansion de la notion de donnée à caractère personnel devrait donc servir la protection de la vie privée. Pourtant, en pratique, les effets de l'expansion demeurent assez relatifs. Au contraire, celle-ci pourrait même avoir tendance à diluer la notion de vie privée dans un vaste ensemble d'informations indirectement personnelles, sans cibler les traitements portant effectivement atteinte aux personnes.

201. Une réduction des informations pouvant circuler librement. En appliquant la notion de donnée à caractère personnel de plus en plus largement, c'est le nombre d'informations pouvant circuler librement qui se réduit. Quel en est l'impact pour les autres libertés ? Les libertés fondées sur l'information, telles que la liberté d'innovation ou les libertés d'expression et d'information, ne sont-elles pas touchées par cette expansion ?

202. Plan. Après avoir étudié les effets marginaux de l'expansion de la notion de donnée à caractère personnel sur la protection de la vie privée (Section I), nous verrons en quoi elle a des effets négatifs sur les libertés liées à l'information (Section II).

---

[698] Art. 1er de la loi du 6 janvier 1978.
[699] N. Ochoa, *Le droit des données personnelles, une police administrative spéciale*, th. Paris I, 2014, p. 436.

SECTION I – LES EFFETS MARGINAUX DE L'EXPANSION SUR LA PROTECTION DE LA VIE PRIVÉE

203. Des doctrines divergentes. L'analyse historique de la construction du droit au respect de la vie privée et du droit des données à caractère personnel a montré que ces matières reposent sur un objectif commun de protection des informations relatives aux personnes[700]. Dès lors, la question des rapports entre la notion de vie privée et celle de donnée à caractère personnel est épineuse. À première vue, la notion de donnée à caractère personnel semble plus large que celle de vie privée puisqu'elle est censée concerner *toute* information relative à une personne alors que la vie privée ne protège que les informations les *plus personnelles*[701]. L'élément distinctif entre ces deux notions réside fondamentalement dans le *lien* entretenu par l'information avec la personne : pour la vie privée, ce lien doit être certain, étroit, et permettre d'enrichir la connaissance d'un tiers, alors que pour les données à caractère personnel, ce rattachement peut être seulement indirect, éventuel, voire incertain ou porter sur une information triviale[702]. En dépit de cette différence, ces deux notions partagent une construction historique complémentaire et un objectif commun[703]. Il semble donc naturel d'attendre d'importants rapprochements.

C'est sans doute pourquoi une opinion doctrinale considère que *la plupart* des données à caractère personnel concernent la vie privée de leur titulaire[704]. À l'inverse, d'autres auteurs affirment que la notion de donnée à caractère personnel est *autonome* vis-à-vis de celle de vie privée car les données à caractère personnel ont vocation à

---

[700] V. *supra*, n° 177.

[701] Monsieur Daniel Gutmann définissait la vie privée comme « un ensemble d'informations personnelles ». Il distinguait toutefois cette notion de celle de donnée à caractère personnel puisque l'adjectif personnel s'entend « en un sens extrêmement vaste, englobant largement le sens restreint que nous avions préféré pour délimiter l'étendue de l'information relevant de la vie privée », D. Gutmann, *Le sentiment d'identité. Étude de droit des personnes et de la famille*, th. Paris II, 2000, LGDJ, n° 259, p. 228 s. et n° 328, p. 277.

[702] Selon certains auteurs, ce n'est pas le lien entre l'information et la personne qui permet de distinguer ces deux notions. En effet, « pour être relative à la vie privée, une information doit concerner la vie personnelle et familiale ; elle est qualifiée par son *contenu*. Pour être personnelle, une information doit seulement être rattachée à une personne ; elle est qualifiée par sa *nature* », v. I. de Lamberterie et J.-H. Lucas (dir.), *Informatique, libertés et recherche médicale*, CNRS, 2001, n° 169. Une telle distinction ne convainc pas puisqu'il est possible de porter atteinte à la vie privée par le traitement d'informations triviales, telles que des métadonnées, v. *infra*, n°s 267 s.

[703] V. *supra*, n°s 163 s.

[704] V. not. D. Chauvet, *La vie privée. Étude de droit privé,* th. Paris-Sud, 2014, n° 524, p. 408 ; E. Derieux, « Vie privée et données personnelle – Droit à la protection et "droit à l'oubli" face à la liberté d'expression », *Les Nouveaux Cahiers du Conseil constitutionnel* 2015, n° 48, p. 21. Selon une opinion doctrinale, le droit à la protection des données personnelles serait absorbé par le droit au respect de la vie privée, v. M. Briat et C. M. Pitrat, « Urgent, concepts à clarifier : protection de la vie privée et des données personnelles », *Droit de l'informatique et des télécoms* 1998, n° 3, p. 13 ; P. Trudel, « La protection de la vie privée dans les systèmes d'information relatifs à la santé. Ajuster les concepts aux réalités des réseaux », in *Les pratiques de recherche biomédicales visitées par la bioéthique*, dir. C. Hervé, B.-M. Knoppers et P. Molinari, Dalloz, 2003, p. 166 s.

couvrir les données se rapportant à la vie privée, à la vie personnelle, ainsi que les données en lien avec la vie professionnelle et la vie publique[705]. Face à ces deux approches apparemment incompatibles, une analyse de l'interprétation par la jurisprudence de ces notions aide à mieux comprendre leurs interactions.

204. Plan. Loin d'être hermétiques, les notions de donnée à caractère personnel et de vie privée maintiennent des liens évidents[706]. Ainsi, lorsque les juridictions sont saisies, elles ont tendance à les interpréter de manière relativement similaire (§ I). Cette similarité témoigne de l'apport marginal de l'expansion de la notion de donnée à caractère personnel à l'égard de la mise en œuvre du droit au respect de la vie privée (§ II).

§ I. Des domaines similaires

205. Plan. Lorsque les juridictions sont saisies de demandes relatives à des informations concernant des personnes physiques, elles basent souvent leurs décisions tant sur le fondement du droit des données à caractère personnel que sur celui du droit au respect de la vie privée[707]. Une telle dualité témoigne de la porosité entre les deux notions en jurisprudence. L'étude du constat de l'assimilation (A) sera suivie par celle de sa mesure (B).

A. Le constat de l'assimilation en jurisprudence

206. Des interprétations jurisprudentielles similaires. Les juridictions n'hésitent pas à rapprocher les notions de donnée à caractère personnel et de vie privée[708]. Cela est particulièrement flagrant dans la jurisprudence du Conseil constitutionnel (1), celle de la Cour de justice de l'Union européenne (2) et celle de la Cour européenne des droits de l'homme (3).

---

[705] V. not. A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, n° 497, p. 220 ; I. de Lamberterie, H.-J. Lucas (dir.), *Informatique, libertés et recherche médicale*, Edition CNRS, 2001, n° 430, p. 169. Pourtant, l'interprétation très large de la notion de vie privée retenue par la Cour européenne des droits de l'homme remet en cause, partiellement au moins, ces théories, v. par ex., B. Teyssié, *Droit des personnes*, 21e éd., LexisNexis, 2019, nos 145 s., p. 138.
[706] I. de Lamberterie et J.-H. Lucas (dir.), *Informatique, libertés et recherche médicale*, CNRS, 2001, n° 157.
[707] Sur la dualité de fondement, v. *supra*, nos 178 s.
[708] M. Clément-Fontaine, « L'union du droit à la protection des données à caractère personnel et du droit à la vie privée », *Légicom* 2017, n° 59, p. 61, spéc. p. 64 s.

1. Les liens dans la jurisprudence du Conseil constitutionnel

207. La protection de la vie privée par le Conseil constitutionnel. Déterminer la qualification juridique du droit au respect de la vie privée – liberté individuelle, liberté personnelle, droit fondamental ou droit subjectif – est une opération complexe[709]. Pourtant celle-ci est essentielle pour déterminer les contours de cette notion et savoir quels intérêts extérieurs peuvent lui être opposés. L'évolution de la jurisprudence du Conseil constitutionnel illustre bien cette difficulté.

Dans un premier temps, le Conseil a reconnu, de manière assez subtile, une protection de la vie privée sur le fondement du droit à la liberté individuelle, garanti par l'article 66 de la Constitution[710]. Malgré cette reconnaissance en demi-teinte, le Conseil constitutionnel a ensuite rejeté, pendant près de deux décennies, les demandes fondées sur un droit constitutionnel au respect de la vie privée[711]. Ce n'est qu'au milieu des années 1990 que la juridiction a repris la démarche initiale et a jugé « que la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle »[712]. Cet élan a définitivement été confirmé par une série de décisions de 1999[713] dans lesquelles il a consacré le droit au respect de la vie privée sur le fondement du *droit à la liberté personnelle,* protégé par l'article 2 de la Déclaration des droits de l'homme et du citoyen[714]. Ainsi, depuis 1999, le Conseil constitutionnel protège le droit au respect de la vie privée sur le fondement de la liberté personnelle.

---

[709] J.-C. Saint-Pau, « Le droit au respect de la vie privée », in *Droits de la personnalité,* dir. J.-C. Saint-Pau, LexisNexis, 2013, n^os^ 1093 s., p. 683 ; D. Chauvet, *La vie privée. Étude de droit privé,* th. Paris-Sud, 2014, n^os^ 10 s., p. 9 s. ; X. Agostinelli, *Le droit à l'information face à la protection civile de la vie privée*, th. Aix-en-Provence, 1994, Librairie de l'Université d'Aix-en-Provence, n^o^ 252, p. 142 s.

[710] Cons. const., 12 janv. 1977, n^o^ 76-75 DC. Le Conseil constitutionnel censure l'unique disposition de cette loi qui autorisait la fouille des véhicules sur le fondement de la liberté individuelle, dont l'article 66 de la Constitution du 4 août 1958 confie la garde à l'autorité judiciaire. Pour une analyse de cette décision, v. P. Gaïa, R. Ghevontian, F. Mélin-Soucramanien, A. Roux et E. Oliva, *Les grandes décisions du Conseil constitutionnel*, 19^e^ éd., Dalloz, 2018, n^o^ 31, p. 471 s.

[711] B. Genevois, *La jurisprudence du Conseil constitutionnel*, Sciences et Techniques Humaines, 1988, n^o^ 352, p. 214. V. not. Cons. const., 14 déc. 1982, n^o^ 82-148 DC, cons. 1 ; Cons. const., 29 déc. 1983, n^o^ 83-164 DC, cons. 35 et 41 ; Cons. const., 26 juill. 1984, n^o^ 84-172 DC, cons. 15 ; Cons. const., 10 et 11 oct. 1984, n^o^ 84-181 DC, cons 25 et 33.

[712] Cons. const., 18 janv. 1995, n^o^ 94-352 DC, cons. 3. V. le commentaire de Monsieur Dominique Rousseau, accueillant favorablement la reconnaissance constitutionnelle de ce droit, D. Rousseau, « Chronique de jurisprudence constitutionnel 1994-1995 », *Revue du droit public et de la science politique en France et à l'étranger* 1996, t. 112, p. 16.

[713] Cons. const., 23 juill. 1999, n^o^ 99-416 DC, cons. 45 ; Cons. const., 9 nov. 1999, n^o^ 99-419 DC, cons. 73 ; Cons. const., 21 déc. 1999, n^o^ 99-422 DC, cons. 52.

[714] Le considérant 45 de la décision du Conseil constitutionnel de juillet 1999 prévoit en effet que « 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 », v. Cons. const., 23 juill. 1999, n^o^ 99-416 DC, cons. 45. Par la même occasion, le Conseil constitutionnel met fin à la compétence exclusive du juge judiciaire en ce qui concerne la protection de la vie privée (découlant de l'article 66 de la Constitution du 4 août 1958) et rend donc légitime l'intervention du juge administratif dans cette matière. Sur cette compétence partagée, v. *infra*, n^os^ 518 s. Pour une étude complète

208. Le rattachement de la protection des données à caractère personnel au droit au respect de la vie privée par le Conseil constitutionnel. Comme pour la reconnaissance du droit au respect de la vie privée, le Conseil constitutionnel a d'abord rattaché la protection des données personnelles au concept de liberté personnelle, puis l'a ensuite liée au concept de liberté individuelle[715]. Finalement et depuis 1999, le Conseil constitutionnel considère que la protection des données à caractère personnel est fondée sur le droit au respect de la vie privée[716]. Ainsi, en droit constitutionnel français, la protection des données personnelles est *assimilée* à celle de la vie privée[717].

Dans ses décisions, le Conseil constitutionnel rattache directement les principes de protection des données à caractère personnel au droit au respect de la vie privée en utilisant fréquemment la formule suivante : « la liberté proclamée par l'article 2 de la Déclaration de 1789 implique le droit au respect de la vie privée. Par suite, 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 »[718]. Cette affirmation illustre le mécanisme d'assimilation entre les deux notions[719] et conforte l'idée selon laquelle la protection des données à caractère personnel ne serait qu'une composante du droit au respect de la vie privée à l'ère numérique[720].

---

du mouvement de constitutionnalisation du droit au respect de la vie privée, V. Mazeaud, « La constitutionnalisation du droit au respect de la vie privée », *Les Nouveaux Cahiers du Conseil constitutionnel* 2015, nº 48, p. 7.

[715] Sur l'évolution des fondements de la protection constitutionnelle en matière de protection des données personnelles, v. N. Ochoa, *Le droit des données personnelles, une police administrative spéciale*, th. Paris I, 2014, p. 408 s.

[716] Cons. const., 23 juillet 1999, nº 99-416 DC, cons. 45 s. Sur cette question, v. N. Ochoa, *Le droit des données personnelles, une police administrative spéciale*, th. Paris I, 2014, p. 413 s.

[717] Ce rattachement a été critiqué par Monsieur Jean Frayssinet qui considérait en 1994 que « restreindre la finalité de la loi de 1978 au seul respect du droit à la vie privée reconnu par l'article 9 du code civil est une erreur d'analyse fréquente, réductrice de la portée et de l'intérêt d'une loi marquant une certaine avance du droit français », v. J. Frayssinet, « Le Conseil constitutionnel et la loi relative à l'informatique, aux fichiers et aux libertés (nº 92-316 DC, 20 janvier 1993) », *Revue française de droit constitutionnel* 1993, nº 14, p. 398. Monsieur Nicolas Ochoa abondait dans ce sens en considérant qu'il arrive que cette protection s'ouvre à d'autres intérêts que la seule protection de la vie privée. L'auteur avait identifié plusieurs décisions dans lesquelles le lien entre la vie privée et les données à caractère personnel était ténu et difficilement plausible, N. Ochoa, *Le droit des données personnelles, une police administrative spéciale*, th. Paris I, 2014, p. 414 s. V. par ex. Cons. const., 16 août 2007, nº 2007-556 DC, cons. 31 ; Cons. const., 22 mars 2012, nº 2012-652 DC, cons. 8, 10 et 11.

[718] V. par ex. Cons. const., 12 juin 2018, nº 2018-765 DC, cons. 47. La formule est encore plus claire lorsque le Conseil constitutionnel considère que le droit au respect de la vie privée « requiert que soit observée une particulière vigilance dans la collecte et le traitement de données à caractère personnel de nature médicale », v. not. Cons. const., 12 août 2004, nº 2004-504 DC, cons. 5.

[719] Le juge constitutionnel considère d'ailleurs « le cadre juridique défini par la loi du 6 janvier 1978 et les pouvoirs reconnus par cette loi à la Commission nationale de l'information et des libertés » comme des garanties nécessaires au respect de la vie privée, v. D. Ribes, « Atteintes publiques et atteintes privées au droit au respect de la vie privée dans la jurisprudence du Conseil constitutionnel », *Les Nouveaux Cahiers du Conseil constitutionnel* 2015, nº 48, p. 35, spéc. p. 43 s. Sur ces liens, v. J.-F. Théry et I. Falque-Pierrotin, « Internet et les réseaux numériques », Conseil d'État, 2 juill. 1998, La Documentation française, 1998, p. 15.

[720] D'ailleurs, le comité de réflexion sur le préambule de la Constitution, présidé par Simone Veil, constatait que la protection des données à caractère personnel « constitue l'une des déclinaisons contemporaines les plus

2. Les liens dans la jurisprudence de la Cour de justice de l'Union européenne

209. Une analyse contextuelle retenue par la jurisprudence de la Cour de justice de l'Union européenne. Fréquemment, la Cour de justice de l'Union européenne associe la protection des données à caractère personnel au droit au respect de la vie privée, alors même que ces droits sont protégés sur deux fondements distincts[721]. Par exemple, la CJUE a considéré, en 2014, que les données de connexion concernent « de manière directe et spécifique la vie privée » et que leur conservation « constitue un traitement des données à caractère personnel »[722]. Pourtant, ces qualifications étaient loin d'être évidentes[723], puisque les données de connexion sont des données techniques générées à l'occasion de l'utilisation d'un service par un utilisateur[724]. Il s'agit notamment de la date, l'heure, la durée, le type d'une communication ainsi que le matériel utilisé. À première vue, il était difficile de qualifier ces données comme des données à caractère personnel puisqu'une date, une heure ou un matériel ne concernent pas une personne. En réalité, cette qualification se justifie par le traitement effectué sur les données, lequel vise l'identification des personnes. C'est également la nature du traitement qui justifiait, pour la CJUE, de retenir l'atteinte à la vie privée. Le caractère systématique de la conservation, la variété des données collectées et la sensibilité des informations pouvant être inférées par ces traitements encourageaient la Cour à retenir une telle approche. Pour toutes ces raisons, elle a considéré qu'une double qualification

---

importantes » du droit au respect de la vie privée, S. Veil (dir.), « Redécouvrir le Préambule de la Constitution. Rapport au président de la République », La Documentation française, déc. 2008, p. 71.

[721] V. *supra*, nº 179.

[722] CJUE, 8 avril 2014, *Digital Rights Ireland Ltd* c. *Minister for communications et al. et Kärntner Landersregierung*, C-293/12 et C-594/12, § 26 s. Cette interprétation a été renouvelée pour « les données relatives au trafic » et les « données de localisation » dans un récent arrêt, CJUE, 6 oct. 2020, *La Quadrature du Net* c. *Premier ministre*, C-511/18, C-512/18 et C-520/18, § 117. V. aussi CEDH, 3 avril 2007, *Copland* c. *Royaume-Uni*, nº 62617/00, § 43 s.

[723] Aux États-Unis, les renseignements de base des abonnés (*basic subscriber information*) sont les données les plus facilement accessibles par les pouvoirs d'enquêtes, v. P. Swire, J. Hemmings et S. Vergnolle, « A mutual legal assistance case study : the United States and France », *Wisconsin International Law Journal* 2017, vol. 42, p. 323 s. [34 WISC. INT. L.J. 323], spéc. p. 333. En France, le Gouvernement Valls II avait publié un article relatif au projet de loi sur le Renseignement dans lequel il considérait que « l'analyse automatique des données de connexion » ne portait pas atteinte à l'anonymat des usagers qui « sera préservé », v. Gouvernement, « Le Vrai/Faux du Gouvernement sur le #PJLRenseignement », 3 avr. 2015.

[724] Le groupe français *Les Exégètes amateurs* définit ces données comme : « les données techniques générées par des fournisseurs de services de communications à l'occasion de l'utilisation de leur service par leurs utilisateurs. On parle souvent de "métadonnées" car ce sont des données à propos d'autres données », Les exégètes amateurs, « Les données de connexion ». Madame Florence Meuris définissait la métadonnée comme « un ensemble structuré de données créées pour fournir des informations sur des ressources numériques », F. Meuris, « Données publiques – "donnée" ouvre-toi ! », *CCE* 2014, nº 2, alerte 10. Pour Madame Marie-Anne Frison-Roche, ce que l'on désigne sous le vocable métadonnées « est le fait de construire des systèmes nouveaux d'information à partir d'éléments constituant des micro-informations disponibles mais éparses, ne prenant de la pertinence et de la valeur qu'au regard d'un usage », M.-A. Frison-Roche, « Penser le monde à partir de la notion de "donnée" », in *Internet, espace d'interrégulation*, dir. M.-A. Frison-Roche, Dalloz, 2016, p. 7.

devait être retenue pour les données de connexion : elles sont des données à caractère personnel et sont aussi des données relatives à la vie privée.

D'autres affaires montrent le caractère fréquent de l'assimilation effectuée par la CJUE entre la notion de donnée à caractère personnel et celle de vie privée[725]. Par exemple, la CJCE avait considéré que le nom d'une personne joint à ses coordonnées téléphoniques ou à des informations relatives à ses conditions de travail ou à ses passe-temps est une donnée à caractère personnel et fait partie du domaine de sa vie privée[726]. Plus récemment, la Cour a retenu que la publication d'informations relatives aux montants perçus par les bénéficiaires d'aides financières caractérise une ingérence dans leur vie privée[727]. La juridiction a considéré que la publication de ces informations portait non seulement atteinte à la protection de leurs données à caractère personnel mais aussi à leur droit au respect de la vie privée. En 2020, la CJUE a été encore plus loin dans cette assimilation en définissant le droit au respect de la vie privée comme « le droit se rapportant à toute information concernant une personne physique identifiée ou identifiable »[728]. Ainsi, la CJUE n'hésite pas à retenir une double qualification pour ces données, sans prendre la peine de distinguer entre la notion de donnée à caractère personnel et celle de vie privée. Plus spécifiquement, elle semble même faire correspondre la notion de vie privée avec celle de donnée à caractère personnel.

3. Les liens dans la jurisprudence de la Cour européenne des droits de l'homme

210. La protection extensive de la vie privée sur le fondement de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme. C'est sans aucun doute dans la jurisprudence de la CEDH que les liens entre les notions de vie privée et de donnée à caractère personnel sont les plus forts. L'article 8 de la Convention européenne de sauvegarde des droits de l'homme prévoit, dans son alinéa premier, que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de

[725] D'ailleurs, pour Madame Christina Koumpli, « les deux notions sont utilisées de façon interchangeable alors qu'elles ne sont pas synonymes », C. Koumpli, *Les données personnelles sensibles. Contribution à l'évolution du droit fondamental à la protection des données à caractère personnel*, th. Paris I, 2019, p. 25.
[726] CJCE, 6 nov. 2003, *Bodil Lindqvist*, C-101/01, § 24 et § 86. Depuis longtemps, la CEDH considère que le nom, « en tant que moyen d'identification personnelle et de rattachement à une famille » concerne la vie privée et familiale, v. CEDH, 25 nov. 1994, *Stjerna* c. *Finlande*, n° 18131/91, § 37.
[727] CJUE, 9 nov. 2010, *Volker und Markus Schecke GbR* et *Hartmut Eifert* c. *Land Hessen*, C-92/09 et C-93/09, § 58.
[728] CJUE, 16 juill. 2020, *Data Protection Commissioner* c. *Facebook Ireland Ltd, Maximillian Schrems,* C-311/18, § 170.

sa correspondance ». La lettre du texte distingue la vie privée de la vie familiale, sans pour autant définir ces notions[729]. D'ailleurs, la CEDH a reconnu, dans plusieurs arrêts, qu'il n'est ni possible, ni nécessaire de chercher à définir de manière exhaustive la notion de vie privée[730]. Cette absence de définition, cumulée à l'interprétation assez stricte de la vie familiale, a encouragé une interprétation souple et étendue de la notion de vie privée. La juridiction a découvert, au fil de ses décisions, les éléments couverts par celle-ci, lesquels incluent des aspects très variés de la vie personnelle des individus[731]. Sans épuiser la notion, ces évolutions dessinent les contours de la vie privée, et ce, dans un perpétuel mouvement[732].

211. Les éléments couverts par la notion de vie privée au sens de la CEDH. Pour la CEDH, la vie privée est une notion manifestement plus large que celle d'intimité puisqu'elle englobe une sphère dans laquelle toute personne peut librement construire sa personnalité et s'épanouir dans ses relations avec les autres et le monde extérieur[733]. La juridiction protège, sur le fondement de l'article 8, les informations liées aux activités professionnelles[734] ou aux activités commerciales[735], ainsi que le droit de vivre en privé, loin de toute attention non voulue[736]. Elle protège également le droit à l'épanouissement personnel[737], que ce soit sous la forme du développement

[729] L'article 8 assure la protection de plusieurs droits, si bien que la CEDH utilise parfois l'expression « volet » pour distinguer parmi les droits, v. CEDH, 12 sept. 2012, *Nada* c. *Suisse*, n° 10593/08, § 154, v. J.-L. Sauron et A. Chartrier, *Les droits protégés par la Convention européenne des droits de l'homme*, Gualino, 2014, n° 434.
[730] CEDH, 16 déc. 1992, *Niemietz* c. *Allemagne*, n° 13710/88, § 29 ; *adde,* CEDH, 25 mars 1993, *Costello-Roberts* c. *Royaume-Uni*, n° 13134/87, § 36. Si, pour la CEDH, il n'existe pas de définition exhaustive de la vie privée, l'Assemblée parlementaire du Conseil de l'Europe a quand même défini, dans le paragraphe 17 de la Résolution 428 adoptée le 23 janvier 1970, la vie privée comme « le droit de mener sa vie comme on l'entend avec un minimum d'ingérence ».
[731] Le droit du travail a contribué au développement de la distinction entre vie privée et vie personnelle, v. P. Waquet, « La vie personnelle du salarié », in *Mélanges J.-M. Verdier,* Dalloz, 2001, p. 513 s. V. déjà, M. Despax, « La vie extraprofessionnelle du salarié et son incidence sur le contrat de travail », *JCP G* 1963, I, chron. 1776. V. aussi, *Rép. civ.* Dalloz, *V°* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), n^os^ 94 s.
[732] Y. Poullet, « Pour une troisième génération de règlementation de protection des données », in *Défis du droit à la protection de la vie privée*, dir. M. Pérez Asinari et P. Palazzi, Bruylant, 2008, p. 38.
[733] V. not. CEDH, 16 déc. 1992, *Niemietz* c. *Allemagne*, n° 13710/88, § 29 ; CEDH, 6 mai 2001, *Bensaïd* c. *Royaume-Uni*, n° 44599/98, § 47 ; I. Roagna, *La protection du droit au respect de la vie privée et familiale par la Convention européenne des droits de l'homme*, Conseil de l'Europe, 2012, p. 15.
[734] CEDH, 16 févr. 2000, *Amann* c. *Suisse*, n° 27798/95, § 65 ; CEDH, 14 mai 2000, *Rotaru* c. *Roumanie*, n° 28341/95, § 43 et CJUE, 9 nov. 2010, *Volker und Markus Schecke GbR* et *Hartmut Eifert* c. *Land Hessen*, C-92/09 et C-93/09, § 59.
[735] CEDH, 16 déc. 1992, *Niemietz* c. *Allemagne*, n° 13710/88, § 29 ; CEDH, 25 juin 1997, *Halford* c. *Royaume-Uni*, n° 20605/92, § 42 s.
[736] CEDH, 24 juill. 2003, *Smirnova* c. *Russie*, n° 46133/99 et n° 48183/99, § 95 ; CEDH, 27 juill. 2004, S*idabras et Džiautas* c. *Lituanie*, n° 55480/00 et n° 59330/00, § 43 ; CEDH, 5 juill. 2011, *Avram et autres* c. *Moldavie*, n° 41588/05, § 36.
[737] V. not. CEDH, 17 févr. 2005, *K.A. et A.D.* c. *Belgique*, n° 42758/98 et n° 45558/99, § 83.

personnel[738], de l'autonomie personnelle[739] ou de la qualité de vie[740]. Plus spécifiquement, la notion de vie privée couvre l'image d'un individu[741], ainsi que les enregistrements vidéo[742]. L'article 8 de la Convention protège très largement les domaines relatifs au sexe tels que l'identité sexuelle[743], l'orientation sexuelle[744] et la vie sexuelle[745]. La notion de la vie privée protège aussi le droit de connaître ses origines[746], la décision d'avoir ou non un enfant[747], les informations relatives à l'identité d'une personne, telles que son état-civil, son statut juridique[748] ainsi que son

---

[738] V. not. CEDH, 6 févr. 2001, *Bensaïd* c. *Royaume-Uni*, nº 44599/98, § 47.
[739] CEDH, 28 mai 2009, *Bigaeva* c. *Grèce,* nº 26713/05, § 22.
[740] CEDH, 29 avr. 2002, *Pretty* c. *Royaume-Uni*, nº 2346/02, § 61.
[741] Pour la CEDH, le droit à l'image bénéficie d'une large protection puisque pour que celui-ci soit considéré effectif, il présuppose en principe le consentement de l'individu dès sa captation et non pas seulement au moment de son éventuelle diffusion au public, CEDH, 27 mai 2014, *De La Flor Cabrera* c. *Espagne*, nº 10764/09, § 31. Pour un rappel de la jurisprudence de la Cour en la matière, v. CEDH, 10 nov. 2015, *Couderc et Hachette Filipacchi Associés* c. *France*, nº 40454/07, § 83. Cette protection s'étend également aux personnes publiques et aux personnes entrées dans la vie publique, CEDH, 21 févr. 2002, *Schüssel* c. *Autriche*, nº 42409/98, § 2 ; v. la série d'arrêts *Von Hannover* [CEDH, 24 juin 2004, *Von Hannover* c. *Allemagne*, nº 59320/00, § 50 s. ; CEDH, 7 févr. 2012, *Von Hannover* c. *Allemagne*, nº 40660/08 et nº 60641/08, § 95 s. ; CEDH, 19 sept. 2013, *Von Hannover* c. *Allemagne*, nº 8772/10, § 41 s.] ; v. aussi CEDH, 4 juin 2009, *Standard Verlags GMBH* c. *Autriche*, nº 21277/05, § 46 s. ; CEDH, 18 janv. 2011, *Mgn Limited* c. *Royaume-Uni*, nº 39401/04, §143 s. Cette protection est également reconnue au bénéfice des personnes « ordinaires », CEDH, 28 janv. 2003, *Peck* c. *Royaume-Uni*, nº 44647/98, § 57 ; CEDH, 17 oct. 2006, *Gourguenidzé* c. *Géorgie*, nº 71678/01, § 40 s. ; CEDH, 13 oct. 2015, *Bremner* c. *Turquie*, nº 37428/06, § 78. Cette protection bénéficie aussi à une personne faisant l'objet de poursuites pénales, CEDH, 11 janv. 2005, *Sciacca* c. *Italie*, nº 50774/99, § 26 s., aux enfants de personnes publiques, CEDH, 17 mars 2016, *Kahn* c. *Allemagne*, nº 16313/10, § 63, mais aussi aux enfants de personnes ordinaires, CEDH, 15 févr. 2009, *Reklos et Davourlis* c. *Grèce*, nº 1234/05, § 34 s. La Cour a également reconnu que la divulgation de l'image d'une personne peut porter atteinte à la vie privée de ses proches, CEDH, 14 juin 2007, *Hachette Filipacchi associés* c. *France*, nº 71111/01, § 46 s. ; CEDH, 25 févr. 2016, *Société de conception de presse et d'édition* c. *France*, nº 4683/11, § 46.
[742] CEDH, 27 mai 2014, *De La Flor Cabrera* c. *Espagne*, nº 10764/09, § 30 s. ; CEDH, 13 oct. 2015, *Bremner* c. *Turquie*, nº 37428/06, § 76.
[743] Sur l'évolution de la jurisprudence de la CEDH en la matière, v. A. Debet, *L'influence de la Convention européenne des droits de l'homme sur le droit civil*, th. Paris II, 2002, Dalloz, nºs 313 s., p. 319 s. V. aussi les nombreuses décisions sur ce thème, par ex., CEDH, 25 mars 1992, *B.* c. *France*, nº 13343/87, § 43 s. ; CEDH, 11 juill. 2002, *Christine Goodwin* c. *Royaume-Uni*, nº 28957/95, § 71 s. ; CEDH, 11 juill. 2002, *I.* c. *Royaume-Uni*, nº 25680/94, § 51 s. ; CEDH, 12 juin 2003, *Van Kück* c. *Allemagne*, nº 35968/97, § 69 s. ; CEDH, 23 mai 2006, *Grant* c. *Royaume-Uni*, nº 32570/03, § 39 s. ; CEDH, 11 sept. 2007, *L.* c. *Lituanie*, nº 27527/03, § 56 s. ; CEDH, 10 mars 2015, *Y. Y.* c. *Turquie*, nº 14793/08, § 56 s. ; CEDH, 6 avril 2017, *Garçon et Nicot* c. *France*, nº 79885/12, nº 52471/13 et nº 52596/13, § 92 s.
[744] L'orientation sexuelle est protégée sur le fondement de l'article 8, de manière autonome mais aussi de manière combinée à l'article 14 (interdiction des discriminations). Sur le fait de prendre en compte l'orientation sexuelle en matière d'adoption, CEDH, 22 janv. 2008, *E.B.* c. *France*, nº 43546/02, § 89 s., ou en matière d'autorité parentale, CEDH, 21 déc. 1999, *Salgueiro Da Silva Mouta.* c. *Portugal*, nº 33290/96, § 23 s., ou en matière de permis de séjour, CEDH, 23 févr. 2016, *Pajić* c. *Croatie*, nº 68453/13, § 61 s., ou en matière de révocation de l'armée, CEDH, 27 sept. 1999, *Lustig-Prean et Beckett* c. *Royaume-Uni*, nº 31417/96 et nº 32377/96, § 64, ou en matière de transmission d'un bail, CEDH, 24 juill. 2003, *Karner* c. *Autriche*, nº 40016/98, § 35 s., ou en matière d'union civile, CEDH, 21 juill. 2015, *Oliari et autres* c. *Italie*, nº 18766/11 et nº 36030/11, § 165 s.
[745] La vie sexuelle fait partie intégrante de la vie privée d'une personne et en constitue un aspect important. Sur ce point, v. CEDH, 22 oct. 1981, *Dudgeon* c. *Royaume-Uni*, nº 7525/76, § 40 s. (relatif à la criminalisation de relations homosexuelles). Cependant, toute pratique sexuelle menée à huis clos ne relève pas nécessairement du domaine de l'article 8, CEDH, 19 févr. 1997, *Laskey, et autres* c. *Royaume-Uni*, nº 21627/93, nº 21628/93 et nº 21974/93, § 36. Comp. CEDH, 17 févr. 2005, *K.A. et A.D.* c. *Belgique*, nº 42758/98 et nº 45558/99.
[746] V. not. CEDH, 7 juill. 1989, *Gaskin* c. *Royaume-Uni*, nº 10454/83, § 39 s. ; CEDH, 13 févr. 2003, *Odièvre* c. *France*, nº 42326/98, § 28 s. ; CEDH, 16 juin 2011, *Pascaud* c. *France*, nº 19535/08, § 48. Sur ce sujet, v. I. Théry, « L'anonymat des dons d'engendrement est-il vraiment "éthique" ? », *Esprit* 2009, p. 133, spéc. p. 139.
[747] V. not. CEDH, 10 avr. 2007, *Evans* c. *Royaume-Uni*, nº 6339/05, § 71 s.
[748] V. not. CEDH, 20 juill. 2010, *Dadouch* c. *Malte*, nº 38816/07, § 47 s. ; CEDH, 27 avr. 2010, *Ciubotaru* c. *Moldavie*, nº 27138/04, § 49.

nom ou prénom[749]. La notion de vie privée protège également les personnes contre les atteintes graves à leur réputation[750] et à leur honneur[751]. De manière plus surprenante, la Cour a également considéré que « des atteintes graves à l'environnement peuvent toucher le bien-être des personnes et les priver de la jouissance de leur domicile de manière à nuire à leur vie privée et familiale »[752]. Ainsi, pour la CEDH, la vie privée est une notion aux facettes multiples, embrassant largement les aspects de l'identité physique, morale, ethnique et sociale d'un individu[753].

212. L'intégration de la protection des données personnelles dans le droit au respect de la vie privée. Les rédacteurs de la Convention étaient loin de penser, en 1950, qu'il faudrait protéger les personnes contre le fichage informatique ou la surveillance numérique. Fort heureusement, l'enrichissement de la liste des droits garantis, effectué par voie d'interprétation judiciaire[754], a préservé la notion de vie privée de tout anachronisme, lui permettant de tenir compte de l'évolution des mœurs et des nécessités sociales[755]. La première trace de la reconnaissance des données personnelles dans la jurisprudence de la CEDH remonte à 1987 lorsqu'elle a été saisie de l'accès à un dossier contenant des informations relatives à l'enfance de Monsieur Torsten Leander. La Cour a reconnu que « le registre secret de la police renfermait sans

---

[749] Pour un rappel de la jurisprudence de la Cour en la matière, v. spéc. CEDH, 7 déc. 2004, *Mentzen* c. *Lettonie*, n° 71074/01. V. aussi CEDH, 22 févr. 1994, *Burghartz* c. *Suisse*, n° 16213/90, § 24 ; CEDH, 25 nov. 1994, *Stjerna* c. *Finlande*, n° 18131/91, § 37. La Cour protège le changement de prénom sur le fondement de l'article 8, CEDH, 25 mars 1992, *B.* c. *France*, n° 13343/87, § 58. La Cour a également protégé le droit pour un enfant victime d'abus sexuels de ne pas voir son nom divulgué dans la presse, CEDH, 17 janv. 2012, *Kurier Zeitungsverlag und Druckerei GMBH* c. *Autriche*, n° 3401/07, § 50 et CEDH, 17 janv. 2012, *Krone Verlag GMBH & Co* c. *Autriche*, n° 33497/07, § 52.

[750] Pour que la protection de l'article 8 s'étende à la réputation, l'attaque doit atteindre un certain niveau de gravité et avoir été effectuée de manière à causer un préjudice à la jouissance personnelle du droit au respect de la vie privée, v. not. CEDH, 9 avr. 2009, *A.* c. *Norvège*, n° 28070/06, § 63 s. ; CEDH, 28 avr. 2009, *Karakó* c. *Hongrie*, n° 39311/05, § 23 s. ; CEDH, 21 sept. 2010, *Polanco Torres et Movilla Polanco* c. *Espagne*, n° 34147/06, § 40 ; CEDH, 7 févr. 2012, *Axel Springer Ag* c. *Allemagne*, n° 39954/08, § 83. Avant de rattacher la protection de la réputation à l'article 8, la Cour utilisait d'autres fondements tels que l'alinéa 2 de l'article 10 et l'article 17 du Pacte international relatif aux droits civils, v. par ex. CEDH, 20 mai 1999, *Bladet Tromsø et Stensaas* c. *Norvège*, n° 21980/93, § 62 s.

[751] V. not. CEDH, 4 oct. 2007, *Sanchez Cardenas* c. *Norvège*, n° 12148/03, § 38 ; CEDH, 9 avr. 2009, *A.* c. *Norvège*, n° 28070/06, § 64.

[752] CEDH, 9 déc. 1994, *López Ostra* c. *Espagne*, n° 16798/90, § 51 ; CEDH, 19 févr. 1998, *Guerra et autres* c. *Italie*, n° 14967/89, § 60.

[753] CEDH, 26 mars 1985, *X et Y* c. *Pays-Bas*, n° 8978/80, § 22 s. ; CEDH, 25 mars 1993, *Costello-Roberts* c. *Royaume-Uni*, n° 13134/87, § 36 ; CEDH, 7 févr. 2002, *Mikulić* c. *Croatie*, n° 53176/99, § 53 ; CEDH, 27 avr. 2010, *Ciubotaru* c. *Moldavie*, n° 27138/04, § 49.

[754] J.-P. Costa, *La Cour européenne des droits de l'homme. Des juges pour la liberté,* 2e éd., Dalloz, 2017, p. 41. Sur le rôle du juge dans l'interprétation de la Convention, v. F. Sudre, « La réécriture de la Convention par la Cour européenne des droits de l'homme », in *Mélanges J.-P. Costa*, Dalloz, 2011, p. 597 s., spéc. p. 599 s. Sur le rôle du juge dans l'effectivité des droits garantis par la CEDH, v. B. Delzangles, « Effectivité, efficacité et efficience dans la jurisprudence de la Cour européenne des droits de l'homme », in *À la recherche de l'effectivité des droits de l'homme*, dir. V. Champeil-Desplats et D. Lochak, Presses Universitaires de Paris Ouest, 2008, p. 41.

[755] F. Sudre (dir.), *Droit européen et international des droits de l'homme*, 14e éd., PUF, 2019, n° 456, p. 697.

contredit des données relatives à la vie privée de M. Leander. Tant leur mémorisation que leur communication, assorties du refus d'accorder à M. Leander la faculté de les réfuter, portaient atteinte à son droit au respect de sa vie privée, garanti par l'article 8 »[756]. Pour autant, la Cour avait prudemment refusé de se prononcer sur « la question de savoir si des droits généraux d'accès à des données et renseignements personnels peuvent se déduire du paragraphe 1 de l'article 8 »[757].

En 1994, la Cour a poursuivi ce mouvement d'assimilation entre la notion de vie privée et celle de donnée personnelle en considérant que les informations identifiantes, notamment le nom ou l'image d'une personne, « en tant que moyen d'identification personnelle et de rattachement à une famille », concernent la vie privée et familiale de celle-ci[758]. En 2000, la CEDH a reconnu que « l'interprétation extensive de la notion de vie privée concorde avec celle de la Convention élaborée au sein du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 »[759]. Ainsi, pour la CEDH, les notions de vie privée et de donnée à caractère personnel sont similaires.

213. Les références à la Convention 108 pour renforcer le droit au respect de la vie privée. L'assimilation de la protection des données personnelles dans le droit au respect de la vie privée s'est confirmée par les nombreuses références, dans les décisions de la CEDH, à la Convention 108[760]. En effet, bien que cette convention soit sans effet direct pour les États membres[761], la CEDH a incorporé, au fil de ses décisions, ses principes dans le droit au respect de la vie privée[762]. Elle a ainsi apporté des garanties au stade de la collecte, de la conservation et de l'exploitation des données, mais aussi lors de leur effacement, de leur destruction et de leur accès par des tiers non

---

[756] CEDH, 26 mars 1987, *Leander* c. *Suède*, n° 9248/81, § 48.
[757] CEDH, 7 juill. 1989, *Gaskin* c. *Royaume-Uni*, n° 10454/83, § 37. La Cour avait tout de même considéré que le dossier personnel d'un enfant, pris en charge par les services sociaux, permet de remplacer les souvenirs et l'expérience vécus par les parents d'un enfant qui n'aurait pas été placé à l'assistance. Ainsi, les informations contenues dans ce dossier relèvent de la vie privée et familiale de l'enfant.
[758] CEDH, 25 nov. 1994, *Stjerna* c. *Finlande*, n° 18131/91, § 37.
[759] CEDH, 16 févr. 2000, *Amann* c. *Suisse*, n° 27798/95, § 65.
[760] Convention pour la protection des personnes à l'égard du traitement des données personnelles, adoptée le 28 janv. 1981. En effet, la Cour de Strasbourg interprète l'article 8 de la CESDH à la lumière des dispositions plus détaillées de la Convention 108, en reconnaissant « à toute personne physique le respect de ses droits et libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant », CEDH, 16 févr. 2000, *Amann* c. *Suisse*, n° 27798/95, § 65.
[761] Le rapport explicatif joint à la Convention confirme que celle-ci n'est pas d'application directe (*self executing*), v. Conseil de l'Europe, « Rapport explicatif de la Convention 108 », 28 janv. 1981, n^{os} 38 et 50.
[762] C'est grâce à une méthode d'interprétation dynamique que la CEDH déduit des dispositions de la CESDH des droits inhérents au respect de ceux textuellement garantis, v. F. Sudre, « À propos du dynamisme interprétatif de la Cour européenne des droits de l'homme », *JCP G* 2001, n° 28, doctr. 335, § 6.

autorisés[763]. Pour la CEDH, la protection des données à caractère personnel se révèle donc être un instrument au service du droit au respect de la vie privée, et une assimilation entre les notions ressort de l'analyse de la jurisprudence[764]. Pour autant, l'assimilation entre ces notions doit être nuancée.

B. La mesure de l'assimilation

214. Plan. Si, dans certains cas, l'assimilation entre la notion de donnée à caractère personnel et celle de vie privée doit être nuancée (1), elle est certaine lorsqu'entrent en jeu des données sensibles (2).

1. Une assimilation à nuancer entre la notion de donnée à caractère personnel et celle de vie privée

215. Nuances au constat de l'assimilation. Bien que réel, le constat de l'assimilation en jurisprudence entre les notions de donnée à caractère personnel et de vie privée doit être relativisé, et cela pour au moins deux raisons. D'une part, les conditions de recevabilité pour saisir ces juridictions ont une forte influence sur le type de contentieux sur lequel elles se prononcent. Par exemple, les seules atteintes que le Conseil constitutionnel est appelé à sanctionner sont celles commises par le législateur[765]. Les conditions très restrictives imposées par les règles de recevabilité des recours devant la CEDH[766] ou la CJUE[767] influent également sur la nature des

[763] La décision de la CEDH du 26 mars 1987 (*Leander* c. *Suède,* n° 9248/81), a été l'un des arrêts fondateurs de l'inclusion de la protection des données personnelles dans le droit au respect de la vie privée. Sur les différents types de garanties apportées par la CEDH en ce qui concerne ces traitements, v. CEDH, « Protection des données personnelles », Fiche thématique, mai 2020.

[764] Comme le note Monsieur Nicolas Ochoa, la CEDH inclut « la protection des données personnelles comme garantie inhérente au respect de la vie privée, quand bien même le champ couvert par le droit des données personnelles serait plus large que celui initialement couvert par la protection de la vie privée. Une telle inclusion, conforme aux canons du droit international public, passe par l'absorption au titre de ses normes de contrôle des premiers fondements directs de la protection des données personnelles en droit international : la Convention n° 108 du Conseil de l'Europe », N. Ochoa, *Le droit des données personnelles, une police administrative spéciale*, th. Paris I, 2014, p. 436. D'ailleurs, la CEDH reconnaît l'importance fondamentale de la protection des données à caractère personnel pour l'exercice du droit au respect de la vie privée, v. not. CEDH, 25 févr. 1997, *Z.* c. *Finlande*, n° 22009/93, § 95 ; CEDH, 27 août 1997, *M. S.* c. *Suède*, n° 20837/92, § 41 ; CEDH, 4 déc. 2008, *S. et Marper* c. *Royaume-Uni*, n° 30562/04 et n° 30566/04, § 103.

[765] D. Ribes, « Atteintes publiques et atteintes privées au droit au respect de la vie privée dans la jurisprudence du Conseil constitutionnel », *Les Nouveaux Cahiers du Conseil constitutionnel* 2015, n° 48, p. 35, spéc. p. 37.

[766] L'effet des conditions très strictes de recevabilité devant la CEDH ne doit pas être minimisé. En effet, la grande majorité des requêtes présentées devant cette juridiction sont déclarées irrecevables ou rayées du rôle (38 480 en 2019, 40 023 en 2018 et 70 356 en 2017), alors que seulement 2 187 requêtes ont donné lieu au prononcé d'un arrêt en 2019, v. CEDH, « Analyse statistique 2019 », janv. 2020. Sur les conditions de recevabilité des requêtes v. F. Sudre (dir.), *Droit européen et international des droits de l'homme*, 14e éd., PUF, 2019, nos 204 s., p. 315 s.

[767] L'article 267 du Traité sur le Fonctionnement de l'Union européenne prévoit en effet que seule une juridiction d'un État membre peut saisir la CJUE d'une demande de question préjudicielle. Sur les conditions de recevabilité de ces questions, v. *Rép. eur.* Dalloz, *Vo* « Compétence judiciaire européenne, reconnaissance et exécution : matières civile et commerciale », par D. Alexandre et A. Huet, 2019 (actu. 2020), nos 10 s.

affaires qui sont présentées devant ces juridictions. D'autre part, si en principe, les justiciables peuvent agir sur le seul fondement de la protection de leurs données à caractère personnel, notamment en cas de traitement illicite de données indirectement identifiantes, plusieurs obstacles entravent une telle action. Tout d'abord, les conditions de responsabilité rendent cette action peu attractive pour les plaideurs[768]. Par ailleurs, le coût et la complexité d'une procédure juridictionnelle, confrontés aux faibles chances de succès d'une telle action, constituent également un frein[769]. En pratique, l'action aura plus de chances d'aboutir lorsque la donnée a été traitée avec d'autres informations (âge, sexe, catégorie socio-professionnelle, sites visités, heures de connexion…), ce qui entraîne la plupart du temps une atteinte à la vie privée de la personne[770].

Ainsi, il est légitime de supposer que les personnes concernées agissent devant les tribunaux pour les atteintes les plus importantes et pas seulement pour des atteintes éventuelles. Ces raisons expliquent sans doute pourquoi la plupart des actions juridictionnelles fondées sur la protection des données à caractère personnel ont également comme fondement le droit au respect de la vie privée[771]. Ainsi, si une assimilation entre les notions est notable dans la jurisprudence, elle doit tout de même être relativisée. D'autant que la dualité de fondement contribue à la distinction, au moins théorique, entre les deux notions[772].

2. Une assimilation certaine entre la notion de donnée sensible et celle de vie privée

216. Les données sensibles, des données relatives à la vie privée. Si des nuances subsistent entre la notion de donnée à caractère personnel et celle de vie privée, celles-ci s'estompent complètement lorsque l'on est en présence de données sensibles. D'ailleurs les définitions de ces notions montrent d'importants recoupements puisque la vie privée a été définie par Monsieur Daniel Gutmann comme « un ensemble de faits, communications ou opinions qui concernent l'individu et dont il serait raisonnable

---

[768] Sur les difficultés pour engager la responsabilité en droit positif, v. *infra*, n^os^ 540 s.
[769] Pour une analyse économique des effets du coût de la procédure sur l'introduction d'actions en justice, v. not. R. Cotter et T. Ulen, *Law and economics*, 6^e^ éd., Addison-Wesley, 2012, p. 242.
[770] V. par ex. CJUE, 8 avril 2014, *Digital Rights Ireland Ltd* c. *Minister for communications et al. et Kärntner Landersregierung*, C-293/12 et C-594/12, § 26 s. V. aussi CEDH, 3 avril 2007, *Copland* c. *Royaume-Uni*, n^o^ 62617/00, § 43 s. cette décision s'intéresse également aux finalités de la conservation des données.
[771] V. *supra*, n^os^ 204 s.
[772] V. *supra*, n^o^ 180.

d'attendre de lui qu'il les considère comme *intimes* ou *sensibles* »[773] et les données sensibles, au sens du règlement européen sont les informations dont le traitement « révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale », ainsi que des « données génétiques, des données biométriques (…), des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique »[774]. Pour ces données, une double qualification juridique est permise : elles entrent assurément dans la notion de vie privée et sont également couvertes par la notion de donnée sensible. Plus spécifiquement, les données relatives à l'origine raciale[775], aux opinions religieuses[776], à l'appartenance syndicale[777], à la santé[778], à

[773] D. Gutmann, *Le sentiment d'identité. Étude de droit des personnes et de la famille*, th. Paris II, 2000, LGDJ, nº 262, p. 230 citant R. Wacks (dir.), *Privacy*. *The concept of privacy*, vol. I., Dartmouth, Aldershot, 1993, p. xvi. Madame Jessica Eynard reprend en substance cette définition en considérant que « la vie privée couvre les informations considérées de façon générale comme privées ainsi que les informations considérées de façon subjective comme particulièrement sensibles », J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 60.

[774] Art. 9 du règlement UE nº 2016/679. Selon le considérant 51 de ce texte, certaines données « sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux [et] méritent une protection spécifique, car le contexte dans lequel elles sont traitées pourrait engendrer des risques importants pour ces libertés et droits ». Sur l'importance de la reconnaissance de l'intimité sexuelle, D. Citron, « Sexual privacy », *The Yale Law Journal* 2019, vol. 128, p. 1874 s. [128 YALE L.J. 1874].

[775] F. Terré et D. Fenouillet, *Droit civil. Les personnes*, 8e éd., Dalloz, 2012, nº 109, p. 119. V. not. TGI Paris, 6 nov. 1974, *Gaz. Pal.* 1975, I, p. 180. Par ailleurs, comme le note Madame Agathe Lepage, la prohibition des discriminations prévues aux articles 225-1 à 225-4 du code pénal contribue indirectement à la protection de la vie privée, v. *Rép. civ.* Dalloz, *Vº* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), nº 55.

[776] Constitue une atteinte au respect dû à la vie privée la révélation publique de la pratique religieuse d'une personne, Cass. civ. 1re, 6 mars 2001, nº 99-10.928, *Bull. civ.* 2001, nº 60, p. 39. Le mariage religieux et le baptême de l'enfant du couple revêtent un caractère privé et la divulgation de cette information constitue une atteinte à leur vie privée, Cass. civ. 1re, 21 mars 2018, nº 16-28.741, *Bull. civ.* 2018, I, nº 56. Sur le secret auquel sont tenus les ministres du culte en ce qui concerne les registres paroissiaux, v. Cass. civ. 1re, 19 nov. 2014, nº 13-25.156, *Bull. civ.* 2014, I, nº 194, p. 39. La CEDH considère que les convictions religieuses de la personne n'ont pas lieu d'apparaître sur sa carte d'identité puisque ce document constitue simplement un document officiel « permettant d'identifier et d'individualiser les personnes en leur qualité de citoyens et dans leurs rapports avec l'ordre juridique de l'État. Les convictions religieuses (…) ne constituent pas une donnée servant à individualiser un citoyen dans ses rapports avec l'État ; non seulement elles relèvent du for intérieur de chacun, mais elles peuvent aussi, comme d'autres données, changer au cours de la vie d'un individu ; leur mention dans un document risque aussi d'ouvrir la porte à des situations discriminatoires dans les relations avec l'administration ou même dans les rapports professionnels », CEDH, 12 déc. 2002, *Sofianopoulos et autres* c. *Grèce*, nº 1988/02, nº 1997/02 et nº 1977/02.

[777] Pour la Cour de cassation, « l'adhésion du salarié à un syndicat relève de sa vie personnelle et ne peut être divulguée sans son accord » et « en cas de contestation sur l'existence d'une section syndicale, le syndicat doit apporter les éléments de preuve utiles à établir la présence d'au moins deux adhérents dans l'entreprise (...), à l'exclusion des éléments susceptibles de permettre l'identification des adhérents du syndicat », Cass. soc., 8 juill. 2009, nº 09-60.011, nº 09-60.031 et nº 09-60.032, *Bull. soc.* 2009, V, nº 180.

[778] Depuis longtemps, la Cour de cassation considère que « la reproduction, dans un but purement commercial, de clichés non autorisés, et l'indication de renseignements sur l'état de santé du mineur, et sur les soins dont il était l'objet » constitue une immixtion intolérable dans sa vie privée, Cass. civ. 2e, 12 juill. 1966, *Bull. civ.* 1966, nº 778. La CEDH reconnaît également une protection pour ces données, v. not. CEDH, 25 févr. 1997, *Z.* c. *Finlande*, nº 22009/93, § 71 ; CEDH, 29 avril 2014, *L. H.* c. *Lettonie*, nº 52019/07, § 56 ; ainsi que la Cour de justice, v. not. CJCE, 8 avr. 1992, *Commission c. Allemagne*, C-62/90, § 23. Ces données sont également protégées au titre du secret médical garanti notamment par l'article L. 1110-4 du code de la santé publique, dès lors que « la santé fait aussi naturellement partie de la sphère de la vie privée », v. *Rép. civ.* Dalloz, *Vº* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), nºs 73 s.

l'orientation sexuelle[779] et à la vie sexuelle[780], ainsi que les données génétiques[781] et les données biométriques[782], entrent dans ces deux notions.

217. Des limites à ces recoupements ? À l'occasion d'un arrêt de 2005, la Cour de cassation a affirmé que « la révélation de l'exercice de fonctions de responsabilité ou de direction au titre d'une quelconque appartenance politique, religieuse ou philosophique ne constitue pas une atteinte à la vie privée »[783]. Cette affirmation a pu laisser penser que des données, pourtant qualifiées comme données sensibles, pourraient être exclues du domaine de la vie privée[784]. En réalité, en visant les « fonctions de responsabilité ou de direction », la Cour de cassation opère une mise en

---

[779] La Cour de cassation a confirmé l'interprétation des juges du fond selon laquelle « la révélation de l'orientation sexuelle de M. X, secrétaire général du Front national » caractérisait une atteinte à sa vie privée (légitime en l'espèce pour l'information du public), Cass. civ. 1re, 9 avr. 2015, nº 14-14.146, *Bull. civ.* 2015, I, nº 85. La cour d'appel de Paris a également considéré que « le terme d'homosexuel définit, au premier chef, l'affinité sexuelle d'une personne envers les personnes de même sexe et relève à l'évidence de la sphère intime protégée par l'article 9 du code civil » et a condamné l'*outing* forcé, v. CA Paris, 21 oct. 2004, nº jurisdata 2004-253278, v. A. Lepage, « Vie privée. Condamnation du "coming out" forcé », *CCE* 2005, nº 3, comm. 48. V. aussi, TGI Paris, réf., 15 mai 2019. Sur la jurisprudence de la CEDH en la matière, v. *supra,* nº 212.

[780] La vie sexuelle fait partie intégrante de la vie privée d'une personne et en constitue un aspect important. Elle est étroitement liée à la vie sentimentale et fait donc partie de l'intimité. Cette protection est particulièrement développée dans la jurisprudence de la CEDH, v. *supra,* nº 212. Les juridictions françaises protègent facilement la vie sentimentale comme un élément de la vie privée, v. sur la diffusion large d'une lettre portant la mention confidentielle ayant pour objet de révéler une situation de concubinage, v. Cass. civ. 1re, 6 oct. 1998, nº 96-13.600, *Bull. civ.* 1998, I, nº 274, p. 191 ; la divulgation des relations entretenues par une jeune femme avec un sportif de renom constitue également une violation de son droit au respect de la vie privée, v. Cass. civ. 2e, 24 avr. 2003, nº 01-01.186, *Bull. civ.* 2003, II, nº 114, p. 98.

[781] Selon Madame Dominique Fenouillet et Monsieur François Terré, « parmi les données inhérentes à la vie privée, une place spéciale doit être faite à l'information génétique qui lui est attachée », v. F. Terré et D. Fenouillet, *Droit civil. Les personnes*, 8e éd., Dalloz, 2012, nº 74, p. 82 s. et nº 109, p. 119. Les données génétiques sont protégées par le droit pénal français notamment depuis la loi nº 2004-800 du 6 août 2004 relative à la bioéthique, *JORF* 7 août 2004, nº 182, p. 14010 (codifiée à l'article 226-5 du code pénal). Pour Madame Agathe Lepage, la répression de ces infractions a pour principale finalité la protection de la vie privée, v. *Rép. civ.* Dalloz, *Vº* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), nº 53. La CEDH protège également les données génétiques au titre de la vie privée, v. not. CEDH, 4 déc. 2008, *S. et Marper* c. *Royaume-Uni*, nº 30562/04 et nº 30566/04, § 86 ; CEDH, 18 avr. 2013, *M. K* c. *France*, nº 19522/09, § 29.

[782] Le Conseil constitutionnel a affirmé que « les données biométriques enregistrées dans ce fichier, notamment les empreintes digitales, étant par elles-mêmes susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu, sont particulièrement sensibles » et que « eu égard à la nature des données enregistrées, à l'ampleur de ce traitement, à ses caractéristiques techniques et aux conditions de sa consultation, les dispositions de l'article 5 portent au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi », Cons. const., 22 mars 2012, nº 2012-652 DC, cons. 10 et 11. La CNIL a également affirmé que le « traitement, sous une forme automatisée et centralisée, de données telles que les empreintes digitales, compte tenu à la fois des caractéristiques de l'élément d'identification physique retenu, des usages possibles de ces traitements et des risques d'atteintes graves à la vie privée et aux libertés individuelles en résultant ne peut être admis que dans la mesure où des exigences en matière de sécurité ou d'ordre public le justifient », v. CNIL, délibération nº 2007-368 portant avis sur un projet de décret en Conseil d'État modifiant le décret nº 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques, *JORF* 10 mai 2008, nº 0109, texte 90. Après quelques hésitations, la CEDH considère également que la conservation d'empreintes digitales (données biométriques) donne lieu « à des préoccupations importantes concernant la vie privée » et « constitue une atteinte au droit au respect de la vie privée », v. CEDH, 4 déc. 2008, *S. et Marper* c. *Royaume-Uni*, nº 30562/04 et nº 30566/04, § 78 s., spéc. § 85.

[783] Cass. civ. 1re, 12 juill. 2005, nº 04-11.732, *Bull. civ.* 2005, I, nº 329, p. 272.

[784] Selon une doctrine majoritaire, « la notion de "vie privée" paraît recouvrir les diverses manifestations positives de l'autonomie de conscience », D. Fenouillet, *La conscience*, th. Paris II, 1993, LGDJ, nº 849, p. 478 s. Selon cette acception, les convictions religieuses, politiques, philosophiques ou morales relèvent bien de la notion de vie privée, v. not. *Rép. civ.* Dalloz, *Vº* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), nº 79.

balance entre deux intérêts concurrents. Ce n'est que face à un éventuel *devoir de transparence*, fondé sur l'obligation de rendre des comptes à l'égard des citoyens, que la vie privée s'efface[785]. Ce devoir de transparence est souvent à la charge de ceux qui « dirigent ou prétendent diriger une institution ou une organisation (franc-maçonnerie comprise) sollicitant (à des degrés et sous des formes variables) adhésions ou suffrages »[786]. Ainsi, en dépit de cette formulation maladroite, la Cour de cassation n'a pas exclu du domaine de la vie privée les convictions politiques, religieuses ou philosophiques ; elle a plutôt opéré un test de proportionnalité entre la protection de ces informations et le droit du public à les connaître[787]. Les données sensibles entrent donc bel et bien dans le domaine de la vie privée et une double protection pour ces données existe.

§ II. Des apports limités

218. La généralisation d'un principe de précaution. L'assimilation opérée par la jurisprudence entre la notion de donnée à caractère personnel et celle de vie privée nous encourage à nous interroger sur les effets de l'expansion de la notion de donnée à caractère personnel sur la protection de la vie privée. Il semble que son principal apport réside dans l'application plus large du droit des données à caractère personnel. Comme l'énonçait déjà Monsieur Pascal Ancel en 1987, « en droit commun, la protection de la personnalité passe surtout par la sanction des atteintes une fois qu'elles se sont produites. La loi de 1978 n'ignore pas ce point de vue : mais, parce qu'on a affaire à des atteintes difficiles à déceler, donc à sanctionner, elle organise aussi – et surtout – un système de prévention des atteintes éventuelles »[788]. En faisant entrer un nombre croissant de données dans le giron de la notion de donnée à caractère personnel, le

---

[785] Sur l'articulation entre la liberté d'information et le droit au respect de la vie privée, v. not. *Rép. civ.* Dalloz, *V°* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), n° 322.
[786] B. Teyssié, *Droit des personnes*, 20e éd., LexisNexis, 2018, n° 232, p. 174.
[787] Monsieur Pascal Ancel confirmait le principe selon lequel « un homme politique ne peut évidemment pas se plaindre de ce qu'on connaisse ses opinions (…) : la presse fait son travail normal en établissant des fiches sur ces personnes. Il est clair en revanche que l'article 33 de la loi n'autoriserait pas une entreprise de presse à tenir un fichier des opinions de ses abonnés – opinions qui font partie de leur vie privée et qui seraient normalement protégées sur le fondement de l'article 9 du code civil », P. Ancel, « La protection des données personnelles : aspects de droit privé français », *RID comp.* 1987, vol. 39, n° 3, p. 609, spéc. p. 620. Pour autant, aujourd'hui, il est courant de voir les entreprises de presse tenir des fichiers sur les visiteurs de leurs sites, v. par ex. G. Dagorn, « Cookies, mouchards : comment vous êtes suivis sur Internet », *Le Monde* 30 mars 2018 ; V. Coquaz, « Les trackers publicitaires ont-ils vraiment été supprimés du site de "Libé" pour les abonnés ? », *CheckNews* 15 nov. 2019.
[788] P. Ancel, « La protection des données personnelles : aspects de droit privé français », *RID comp.* 1987, vol. 39, n° 3, p. 609, spéc. p. 614. Sur l'évolution du régime issu du droit des données à caractère personnel, v. *infra*, n°s 304 s.

principe de prévention des atteintes éventuelles aux personnes s'applique donc plus largement. Monsieur Pascal Ancel poursuivait son analyse en considérant que « le traitement de ces données, parce qu'il les rend aisées à retrouver, à rapprocher, à consulter, à transmettre… peut faire craindre des utilisations abusives. Mais ces abus ne présentent, heureusement, aucun caractère de certitude, et il n'y aurait pas de raison de mettre en œuvre une mesure préventive sur le fondement du droit commun »[789]. Ainsi, le traitement de ces données ne présente pas un risque tel que les mesures préventives prévues au second alinéa de l'article 9 du code civil et à l'article 809 du code de procédure civile soient nécessaires[790]. Pour autant, des mesures d'encadrement plus souples, notamment celles prévues par le droit des données à caractère personnel, doivent être mises en place. La question sous-jacente est évidement celle de savoir si le principe de précaution et l'application étendue du droit des données personnelles servent la protection de la vie privée et s'ils contribuent à l'effectivité de la protection des personnes.

219. Les effets de la distension du lien entre la donnée et la personne. En apparence, dès lors que toute information se rapportant à une personne entre dans la notion de donnée à caractère personnel, il est possible de considérer que la protection de la vie privée est garantie[791]. En réalité, une telle affirmation apparaît relativement simpliste et éclipse la réalité de la protection résultant du droit des données à caractère personnel.

Tout d'abord, l'expansion de la notion de donnée à caractère personnel a tendance à *banaliser* les traitements de données. Une telle banalisation est loin d'être neutre pour la protection des personnes. Elle engendre une sorte de résignation des personnes à l'égard de la collecte, quasi-automatique, d'un nombre toujours plus conséquent de leurs données[792]. Elle rend les traitements de données, même les plus intrusifs, de plus en plus acceptables. En effet, les personnes sont si régulièrement

[789] P. Ancel, « La protection des données personnelles : aspects de droit privé français », *RID comp.* 1987, vol. 39, n° 3, p. 609, spéc. p. 618.
[790] Pour une analyse sur ces mesures, v. not. D. Chauvet, *La vie privée. Étude de droit privé,* th. Paris-Sud, 2014, n^os^ 472 s., p. 376 s. ; *Rép. civ.* Dalloz, *V°* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), n^os^ 236 s.
[791] Le droit des données à caractère personnel prévoit une série de principes favorisant la protection de la vie privée (tels que la minimisation, la sécurité ou encore le principe de pertinence).
[792] Pour une analyse de ces questions, v. D. Solove, « Privacy self-management and the consent dilemma », *Harvard Law Review* 2013, vol. 126, p. 1880 s. [126 HARV. L. REV. 1880].

sollicitées pour consentir à la collecte de leurs données qu'elles cliquent inlassablement jusqu'au moment où elles peuvent accéder au contenu souhaité.

Par ailleurs, l'expansion de la notion met sur le même plan toutes les formes d'atteintes aux personnes et tend ainsi à diluer la protection des personnes[793]. En effet, dès lors que les personnes sont sollicitées quels que soient les effets du traitement, il leur est plus difficile de distinguer les traitements les plus dangereux des traitements anodins.

Enfin, l'expansion de la notion de donnée à caractère personnel distend le lien entre le traitement d'une donnée et l'atteinte à la personne. L'assouplissement de ce lien rend l'application du droit des données personnelles plus complexe à comprendre, tant pour les responsables du traitement que pour les personnes concernées. Il semble effectivement difficile de justifier, en l'absence de traitement particulier, l'inclusion dans le giron de la protection des personnes d'une suite de chiffres[794], d'une date, d'une poubelle publique connectée[795] ou d'un arbre[796]. À ces effets s'ajoute également le fait que le droit des données à caractère personnel accorde une protection limitée des personnes.

220. Une protection limitée des personnes. Contrairement à une conception répandue, la protection résultant du droit des données à caractère personnel est relative[797]. En effet, le but inavoué mais réel du droit des données à caractère personnel[798] est de rendre licites les traitements de ces données[799]. En contrepartie du pouvoir de traiter des données à caractère personnel, les responsables du traitement sont astreints à respecter certaines règles. Ces règles incluent notamment des obligations d'information sur les traitements opérés, des règles concernant la sécurité

---

[793] Comme le remarquait très justement Madame Laure Marino, le risque de cette extension notionnelle est de « noyer » les droits de la personnalité avec « un énorme élargissement des notions », L. Marino, « Les nouveaux territoires des droits de la personnalité », *Gaz. Pal.* 2007, nº 139, p. 22, § 12.
[794] L'adresse IP est, par nature, une suite de chiffres, v. *supra,* nº 186.
[795] Le poids des déchets pourrait renseigner sur la consommation des foyers.
[796] Sur les arbres remarquables et leur qualification par des agents de la CNIL, v. *supra,* nº 149.
[797] V. *infra*, nºs 297 s.
[798] Cette dichotomie entre le but caché et l'objectif affiché se retrouve dans d'autres domaines. Des auteurs remarquaient justement que « les règles, nombreuses en droit de la consommation, qui prescrivent une information obligatoire, présument-elles que les consommateurs sont des superhéros capables de tenir compte de toute cette information ? Comme cela n'est pas réaliste, il semble que ces règles servent en réalité un but autre que la protection effective des consommateurs », A. Alemanno, G. Helleringer et A.-L. Sibony, « Brève introduction à l'analyse comportementale du droit », *D.* 2016, p. 911, citant, pour une critique des obligations d'information dans une perspective comportementale, O. Bar-Gill, *Seduction by Contract*, OUP, 2012. Pour une discussion de cette dichotomie dans le contexte européen, v. not. A.-L. Sibony et G. Helleringer, « EU consumer protection and behavioural sciences : revolution or reform ? », in *Nudge and the law : a european perspective,* dir. A. Alemanno et A.-L. Sibony, Hart Publishing, 2015, p. 209 s.
[799] Sur les conditions de licéité des traitements de données, v. *infra*, nºs 324 s.

des données, et reconnaît des droits aux personnes concernées. En pratique, les obligations d'information se matérialisent souvent par des bandeaux surgissant sur les pages des sites Internet consultés, occultant la plupart du contenu, et contraignant l'utilisateur à accepter ou abandonner sa visite[800]. Quant aux droits des personnes, leur exercice est souvent si complexe et contraignant qu'il rebute l'utilisateur à les exercer pleinement. Pourtant, ces droits sont censés contrebalancer le pouvoir de traiter les données accordé aux responsables du traitement. Ainsi, l'application généralisée de la notion de donnée à caractère personnel crée une illusion de protection dont l'effet pervers est de produire exactement l'inverse : les personnes concernées pensent que leurs données personnelles « sont protégées » alors même qu'elles peuvent être traitées pour des finalités unilatéralement déterminées par le responsable du traitement[801]. Ce système est à rebours de celui mis en place par l'article 9 du code civil lequel sanctionne les atteintes à la vie privée et protège donc les personnes contre des investigations et divulgations non autorisées[802]. Ainsi, l'inclusion d'un nombre croissant de données dans le domaine de la donnée à caractère personnel a un apport plutôt relatif, voire contre-productif, sur la protection de la vie privée. La plupart des traitements de données qui sont effectivement relatifs aux personnes entrent d'ores et déjà dans la conception élargie de la vie privée. En revanche, l'expansion de la notion de donnée à caractère personnel produit des effets négatifs dans d'autres matières, notamment lorsqu'il est question de libertés liées à l'information.

---

[800] À ce propos, la conformité au droit des données personnelles des bandeaux informant sur l'usage des cookies a fait l'objet de nombreux débats. Pour un aperçu des évolutions, v. W. Maxwell et C. Zolynski, « Protection des données personnelles », *D.* 2020, p. 1262, nº 3. Plusieurs études ont montré l'influence du design des bandeaux de cookies sur l'obtention du consentement, v. not. C. Utz, M. Degeling, S. Fahl, F. Schaub et T. Holz, « (Un)informed consent : studying GDPR consent notices in the field », *CCS'* nov. 2019, Londres ; M. Nouwens, I. Liccardi, M. Veale, D. Karger et L. Kagal, « Dark patterns after the GDPR : scraping consent pop-ups and demonstrating their influence », *CHI'* avr. 20, Honolulu.

[801] Pour une analyse de la variété d'intérêts permettant de justifier un traitement de donnée à caractère personnel, v. *infra*, nºs 325 s. Cette impression de protection doit être mise en relation avec les conditions dans lesquelles le consentement est obtenu. Monsieur Pierre Trudel rappelait justement les limites de l'approche fondée sur le consentement des personnes : « alors qu'au départ, on poursuivait la finalité d'assurer la protection de la vie privée, on s'est retrouvé avec un système qui permet d'obtenir toutes sortes d'informations à la condition d'avoir un consentement », v. P. Trudel, « La protection de la vie privée dans les systèmes d'information relatifs à la santé. Ajuster les concepts aux réalités des réseaux », in *Les pratiques de recherche biomédicales visitées par la bioéthique*, dir. C. Hervé, B.-M. Knoppers et P. Molinari, Dalloz, 2003, p. 168. Par ailleurs, et comme le rappelait Monsieur Emmanuel Netter, « Rédiger de belles politiques de confidentialité ou de beaux contrats ne sert à rien si personne ne les lit. (…) Pour ralentir la course folle vers un consentement mécanique et vide de signification, le législateur fait assaut d'imagination : un exemple bien connu – et à ne pas suivre – est celui des mentions manuscrites laborieusement recopiées par les cautions, supposées les pénétrer du sens de leur engagement tandis que les minutes s'écoulent. En ligne plus encore qu'ailleurs, l'utilisateur a tendance à foncer comme un taureau furieux vers l'instant où il pourra bénéficier du service. » v. not. E. Netter, « Sanction à 50 millions d'euros : au-delà de Google, la CNIL s'attaque aux politiques de confidentialité obscures et aux consentements creux », *Dalloz IP/IT* 2019, p. 165.

[802] P. Kayser, « Aspects de la protection de la vie privée dans les sociétés industrielles », in *Mélanges G. Marty*, Université des sciences sociales de Toulouse, 1978, p. 725 s., nº 3, spéc. p. 727.

SECTION II – LES EFFETS NÉGATIFS DE L'EXPANSION SUR LES LIBERTÉS LIÉES À L'INFORMATION

221. La protection des données à caractère personnel, un droit fondamental. Le droit des données personnelles a glissé d'un simple droit subjectif, outil « de sauvegarde et de promotion de valeurs plus fondamentales »[803], vers une valeur en soi, et a été élevé au titre de droit autonome et qualifié par certains auteurs comme droit fondamental[804]. En dépit des critiques formulées à l'égard d'une telle reconnaissance[805], ce droit est désormais protégé par l'article 8 de la Charte des droits fondamentaux de l'Union européenne[806]. La fondamentalisation du droit des données à caractère personnel est loin d'être anodine dès lors qu'elle implique que ce droit peut restreindre d'autres droits fondamentaux, tels que la liberté d'information, la liberté d'opinion ou la liberté d'expression[807].

---

[803] Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », in *État de droit et virtualité*, dir. K. Benyekhlef et P. Trudel, Thémis, 2009, p. 157 s., spéc. p. 168 s.

[804] S. Peyrou, « La protection des données à caractère personnel : un droit désormais constitutionnalisé et garanti par la CJUE », in *La protection des droits fondamentaux dans l'Union européenne*, dir. R. Tinière et C. Vial, Bruylant, 2015, p. 213 s. ; E. Debaets, *Le droit à la protection des données à caractère personnel. Recherche sur un droit fondamental*, th. Paris I, 2014 ; C. Chevallier-Govers, « Le droit à la protection des données à caractère personnel : un droit fondamental du XXIe siècle ? » in *Enjeux et perspectives des droits de l'homme. L'Odyssée des droits de l'homme,* t. 3, dir. J. Ferrand et H. Petit, L'Harmattan, 2003, p. 79. Sur les qualifications juridiques du droit au respect des données personnelles, v. M. Bénéjat, « Les droits sur les données personnelles », in *Droits de la personnalité,* dir. J.-C. Saint-Pau, LexisNexis, 2013, nº 926, p. 561 s.

[805] Par exemple, pour Monsieur Emmanuel Dreyer, « il existe un mouvement, pernicieux, consistant à galvauder les droits fondamentaux. Il consiste à qualifier de la même façon le droit et ses démembrements. Il en résulte une augmentation du nombre des droits concernés qui ne méritent pas toujours leur qualification. La Charte des droits fondamentaux de l'Union européenne en fournit la meilleure illustration. À titre d'exemple, au lieu de rattacher la protection des données à caractère personnel au droit au respect de la vie privée, l'article 8 de cette Charte lui consacre des développements spécifiques. Les droits d'accès aux fichiers et de rectification sont, bien entendu, essentiels mais constituent-ils, pour autant, des droits fondamentaux ? », E. Dreyer, « La fonction des droits fondamentaux dans l'ordre juridique », *D.* 2006, p. 748, nº 11. Pour un exposé des travaux qualifiant le droit des données personnelles comme un droit fondamental, v. C. Koumpli, *Les données personnelles sensibles. Contribution à l'évolution du droit fondamental à la protection des données à caractère personnel*, th. Paris I, 2019, p. 30 s. En France il s'agit, tout au moins, d'un droit en voie de « fondamentalisation », notamment parce que le Conseil constitutionnel ne lui reconnaît pas (encore ?) une existence autonome, malgré les demandes pressantes des Présidents de la CNIL, v. not. J.-M. Pastor, « La CNIL veut inscrire la protection des données dans la Constitution », *AJDA* 2008, p. 964.

[806] Charte des droits fondamentaux de l'Union européenne, *JOUE* 30 mars 2010, C-83/02, p. 389 s. Dès septembre 1999, le groupe G29 avait souhaité voir reconnaître la protection des données à caractère personnel comme un droit fondamental autonome, lequel « dépasse, en effet, la question de la vie privée et doit être régi par des principes particuliers tant il s'agit, en réalité, de protéger, au titre des leurs données à caractère personnel notamment dans le cadre de la société de l'information, l'identité des personnes concernées », v. CNIL, *Rapport d'activité 2000,* La Documentation française, 2001, p. 187. Le considérant premier du règlement européen rappelle d'ailleurs que « la protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental ».

[807] Art. 52 de la Charte des droits fondamentaux de l'Union européenne, *JOUE* 30 mars 2010, C-83/02, p. 389 s. Comme le rappelait justement Madame Danièle Lochak, « si des bornes peuvent être légitimement posées à l'exercice des libertés, c'est dans la stricte mesure où elles sont nécessaires pour préserver les fondements de la vie en société et rendre possible la coexistence harmonieuse entre ses membres. La notion d'équilibre, qui doit guider l'arbitrage entre des exigences opposées, est ici fondamentale, mais elle est aussi très incertaine : car il faut décider non seulement de ce que l'on va placer dans chacun des plateaux de la balance, mais encore, par une évaluation forcément arbitraire, du poids respectif de ce qu'on y a placé », D. Lochak, *Les droits de l'homme*, La Découverte, 2018, p. 92 s. Comme le remarque Madame Nathalie Mallet-Poujol, la protection des données à

222. Les conséquences de l'expansion de la notion de donnée à caractère personnel sur les autres libertés. Lorsqu'une donnée est qualifiée de donnée à caractère personnel, les traitements qui sont effectués sur elle sont soumis aux règles du droit des données à caractère personnel. Ces règles encadrent les traitements effectués sur ces données et empêchent leur accès par des tiers non autorisés. Pour le dire simplement, « les informations à caractère personnel ne sont librement disponibles, ni dans leur collecte, ni dans leur traitement »[808]. Dans cette configuration, le droit des données à caractère personnel a une influence non seulement sur les informations sur lesquelles il est possible de s'exprimer, mais aussi sur celles auxquelles il est possible d'accéder[809]. L'expansion de la notion de donnée à caractère personnel n'aboutit-elle pas à une restriction indue de la liberté de circulation des informations, laquelle est essentielle à l'exercice d'autres droits fondamentaux ?

223. Plan. L'expansion de la notion de donnée à caractère personnel a des conséquences non négligeables pour l'exercice d'autres droits fondamentaux. Elle a des effets, notamment sur la liberté d'information (§ I) et sur la liberté d'expression (§ II).

§ I. Les effets sur la liberté d'information

224. Plan. La liberté d'information a longtemps été considérée comme une composante de la liberté d'expression. Depuis quelques décennies, elle a pris son indépendance et bénéficie d'une protection autonome (A). Elle se place donc en concurrence avec d'autres droits et libertés avec lesquelles elle doit s'articuler[810]. À ce titre, elle entretient des rapports indéniables avec le droit des données à caractère personnel (B).

---

caractère personnel « ne peut donc pas être opposée au droit à l'information avec la même intransigeance que le droit à la vie privée, d'autant que la collecte des données obéit souvent à des impératifs de service public ou de rationalisation de la gestion et que le stockage numérique est mis en place pour faciliter l'accès à la donnée personnelle », N. Mallet-Poujol, « Protection des données personnelles et droit à l'information », *Légicom* 2017, n° 59, p. 49, spéc. p. 53.

[808] *Le Lamy droit du numérique*, *V°* « Des informations qui ne sont pas disponibles », § 356, actu. 2018, dir. M. Vivant.

[809] La référence à la libre circulation de l'information dans les titres de la directive CE n° 95/46 et du règlement UE n° 2016/679 est trompeuse. Elle laisse croire que les données peuvent circuler librement alors que ces textes visent plutôt à garantir un seuil de protection commun sur le territoire de l'Union européenne afin d'éviter les entraves à la circulation des données.

[810] X. Agostinelli, *Le droit à l'information face à la protection civile de la vie privée*, th. Aix-en-Provence, 1994, Librairie de l'Université d'Aix-en-Provence, n° 84, p. 70.

A. La protection de la liberté d'information

225. Le principe est la liberté ; l'interdiction est l'exception. La liberté consiste, selon l'article 4 de la Déclaration des droits de l'homme et du citoyen, « à pouvoir faire tout ce qui ne nuit pas à autrui ». Appliqué aux informations, ce principe garantit leur libre circulation : chacun peut librement s'en emparer, les analyser et les interpréter[811], tant que ces traitements ne nuisent pas à autrui. C'est pourquoi la liberté d'information implique, sous certaines limites, le libre accès du public à l'information et la libre circulation des supports de l'information[812]. Ce principe est l'un des piliers essentiels de toute société démocratique[813], notamment parce qu'il est déterminant pour rendre effectif le droit de recevoir et de diffuser des informations[814]. Par opposition, seules certaines informations doivent voir leur circulation restreinte, restriction qui doit être fondée sur une justification prévue par la loi et être proportionnée à l'objectif poursuivi[815].

226. L'affirmation de la liberté d'information. Longtemps, la liberté d'information était protégée sur le fondement de la liberté d'expression. Elle en est le corollaire car cette dernière « ne prend sa véritable dimension que si elle a un destinataire »[816]. Ainsi, l'article 19 de la Déclaration universelle des droits de l'homme prévoit que « tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit ». L'article 10-1 de la CESDH, dont la rédaction est similaire, garantit également une telle liberté de communication. En France, à partir

---

[811] Le dictionnaire de l'Académie française définit libre comme « qui peut s'exercer sans entrave, qui n'est pas soumis à restriction », *Dictionnaire de l'Académie française*, 9e éd., *Vo* « Libre », sens III.3. Dans son livre *Le future des idées,* Monsieur Lawrence Lessig explique qu'une « ressource est "libre" si, premièrement, on peut l'utiliser sans demander d'autorisation à personne, ou si, deuxièmement, cette autorisation est accordée sans contrepartie », L. Lessig, *The future of ideas : the fate of the commons in a connected world,* Random House, 2001, p. 12. Pour un bref exposé du principe de libre circulation, v. aussi, *supra,* no 77.

[812] F. Sudre (dir.), *Droit européen et international des droits de l'homme*, 14e éd., PUF, 2019, no 540, p. 813.

[813] F. Brocal von Plauen, *Le droit à l'information en France*, th. Lyon II, 2004 ; F. Cate, « The changing face of privacy protection in the European union and the United States », *Indiana Law Review* 1999, vol. 33, p. 173 s. [33 IND. L. REV. 173], spéc. p. 174.

[814] L. Favoreu *et al.*, *Droit des libertés fondamentales*, 7e éd., Dalloz, 2015, no 623, p. 529.

[815] F. Sudre, « Le contrôle de proportionnalité de la Cour européenne des droits de l'homme. De quoi est-il question ? », *JCP G* 2017, no 11, doctr. 289, § 3.

[816] X. Agostinelli, *Le droit à l'information face à la protection civile de la vie privée*, th. Aix-en-Provence, 1994, Librairie de l'Université d'Aix-en-Provence, no 80, p. 69.

des années 1980, la liberté d'information a pris son autonomie grâce aux lois sur la communication et aux décisions du Conseil constitutionnel s'y rattachant[817].

227. La transparence, moteur de la liberté d'information. Cette autonomisation de la liberté d'information s'inscrit, en réalité, dans un mouvement plus large, lequel vise à favoriser la transparence et l'information des personnes. De nombreux exemples illustrent ce mouvement : l'augmentation des obligations d'information dans tous les domaines du droit[818] ou le renforcement des obligations de transparence démocratique[819]. Depuis le siècle des Lumières, la transparence se manifeste assurément comme synonyme de découverte, de compréhension, de révélation et d'illumination[820]. À partir de la fin des années 1970, elle est le moteur de nouveaux droits[821]. Par exemple, la loi du 17 juillet 1978[822], animée par l'esprit de l'article 15 de la Déclaration des droits de l'homme et du citoyen, aux termes duquel « la Société a droit de demander compte à tout agent public de son administration », reconnaît le droit des administrés à l'information en ce qui concerne la liberté d'accès aux documents administratifs[823]. Ce mouvement de reconnaissance du droit d'accès à l'information s'est encore amplifié, notamment avec l'adoption du droit d'accès à l'information médicale[824] et avec la consécration du droit d'accès aux informations

---

[817] Cons. const., 11 oct. 1984, nº 84-181 DC, cons. 38 ; Cons. const., 18 sept. 1986, nº 86-217 DC, cons. 11. Par ailleurs, l'article L. 300-1 du code des relations entre le public et l'administration garantit, en ce qui concerne l'accès aux documents administratifs, la liberté d'information. Le Conseil constitutionnel a d'ailleurs récemment consacré l'accès aux documents administratifs comme un droit constitutionnel, Cons. const., 3 avr. 2020, nº 2020-834 QPC, cons. 8. La Charte de l'environnement protège, dans son article 7, le droit « d'accéder aux informations relatives à l'environnement détenues par les autorités publiques et de participer à l'élaboration des décisions publiques ayant une incidence sur l'environnement », v. loi constitutionnelle nº 2005-205 du 1er mars 2005 relative à Charte de l'environnement, *JORF* 2 mars 2005, nº 51, texte 2.

[818] En droit de la santé, les patients doivent être informés avant de consentir librement, v. not. C. Cousin, *Vers une redéfinition de l'acte médical*, th. Rennes I, 2016, nos 414 s., p. 214 s. ; en droit des contrats, des obligations d'information pèsent sur les contractants, v. not. M. Fabre-Magnan, *Essai d'une théorie de l'obligation d'information dans les contrats*, th. Paris I, 1992, LGDJ ; en droit financier les obligations d'information pèsent sur les émetteurs, les intermédiaires financiers et les investisseurs, v. J. Chacornac, *Essai sur les fonctions de l'information en droit des instruments financiers,* th. Paris II, 2012, Dalloz.

[819] B. Mathieu et M. Verpeaux (dir.), *Transparence et vie publique. Neuvième printemps du droit constitutionnel*, Dalloz, 2015.

[820] D'ailleurs, pour Jean-Jacques Rousseau, « la transparence est la vertu des belles âmes ». V. sur la transparence et la démocratie, É. Zoller, « Transparence et démocratie : généalogie d'un succès », in *Transparence, démocratie et gouvernance citoyenne,* dir. G. Guglielmi et É. Zoller, Éd. Panthéon-Assas, 2014, p. 13 s. ; V. Marbillard, *Les effets de la transparence sur la confiance des citoyens. Clarification conceptuelle et étude de cas empire au niveau local*, th. Lausanne, 2019, p. 13 s.

[821] F. Brocal von Plauen, *Le droit à l'information en France*, th. Lyon II, 2004, p. 24 ; J.-D. Bredin, « Secret, transparence et démocratie », *Pouvoirs* 2001, nº 97, p. 5.

[822] Loi nº 78-753 du 17 juill. 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal, *JORF* 18 juill. 1978, nº 0166, p. 2851.

[823] Sur l'histoire de ce mouvement v. *Rép. cont. adm.* Dalloz, *Vº* « Communication des documents administratifs », par A. Lallet et P. Nguyen Duy, 2019, nos 2 s. ; H. Verdier et S. Vergnolle, « L'État et la politique d'ouverture en France », *AJDA* 2016, p. 92.

[824] Ce droit est prévu depuis 2002 à l'article L. 1111-7 du code de la santé publique. Pour une analyse du dossier médical, v. J. Bonneau, « L'accès au dossier médical », *Gaz. Pal.* 2003, nº 127, p. 3 ; N. Vignal, « L'accès au

environnementales par la Charte de l'environnement de 2004[825]. Si la liberté d'information s'est progressivement affirmée comme un droit autonome, elle demeure une composante vitale à plusieurs autres libertés.

228. Une liberté cardinale. La liberté d'information est entendue largement puisqu'elle ne se définit pas seulement par le contenu de l'information, sa qualité ou son importance, mais aussi par son mode de formulation[826]. Ainsi, elle protège non seulement la *substance* des informations exprimées mais aussi leur *mode* de diffusion. Plus largement, elle garantit au public le droit de *recevoir* une information pluraliste[827]. C'est ce qui explique qu'elle est souvent présentée comme le pendant de la liberté d'expression, puisqu'elle en serait la source[828]. Il est vrai que sans elle, la liberté d'expression ne peut pas exister. En effet, en garantissant la libre circulation de l'information, on évite les systèmes de censure, lesquels entravent immanquablement la possibilité de s'exprimer[829]. La liberté d'information entretient également des liens avec la liberté de pensée dès lors qu'elle garantit aux personnes le droit d'accéder à une information libre, pluraliste, transparente et indépendante[830]. Un tel accès permet aux personnes une confrontation de leurs idées, laquelle contribue à la formation des convictions personnelles. La liberté d'information entretient également des rapports subtils avec le droit des données à caractère personnel.

---

dossier médical », *LPA* 19 juin 2002, nº 122, p. 19. Pour une analyse de l'interaction entre le droit d'accès aux documents administratifs et l'accès à l'information médicale, v. S. Dyens, « L'accès aux documents de gestion des agents des collectivités territoriales : entre transparence et confidentialité », *AJ Collectivités territoriales* 2011, p. 387.

[825] Art. 7 de la Charte de l'environnement. Pour une analyse du domaine de cette charte, v. not. F. Brunet, « Le champ d'application de la Charte de l'environnement », *AJDA* 2016, p. 1327.

[826] F. Sudre (dir.), *Droit européen et international des droits de l'homme*, 14e éd., PUF, 2019, nº 540, p. 812.

[827] La CEDH a largement contribué à la protection du pluralisme de l'information, v. not. CEDH, 17 juill. 2001, *Association Ekin* c. *France*, nº 39288/98, § 56, décision dans laquelle la CEDH affirme que la liberté d'expression « vaut non seulement pour les "informations" ou "idées" accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui heurtent, choquent ou inquiètent. Ainsi le veulent le pluralisme, la tolérance et l'esprit d'ouverture sans lesquels il n'est pas de "société démocratique" ». Le Conseil constitutionnel a également consacré le pluralisme comme objectif de valeur constitutionnelle, v. Cons. const., 11 oct. 1984, nº 84-181 DC, cons. 38.

[828] La plupart des manuels relatifs aux droits de l'homme et aux libertés fondamentales la présente toujours comme une de ses composantes, v. F. Sudre (dir.), *Droit européen et international des droits de l'homme*, 14e éd., PUF, 2019, nº 539, p. 810 ; L. Favoreu *et al.*, *Droit des libertés fondamentales*, 7e éd., Dalloz, 2015, nº 623, p. 529 ; S. Hennette-Vauchez et D. Roman, *Droits de l'Homme et libertés fondamentales*, 4e éd., Dalloz, 2020, nº 493, p. 370.

[829] J.-B. Amadieu, « Nos censures au miroir de l'Index librorum prohibitorum », *Raisons politiques* 2016, nº 63, p. 67.

[830] X. Agostinelli, *Le droit à l'information face à la protection civile de la vie privée*, th. Aix-en-Provence, 1994, Librairie de l'Université d'Aix-en-Provence, nº 82, p. 69.

B. Les rapports entre la liberté d'information et le droit des données à caractère personnel

229. La donnée à caractère personne ne circule pas librement. Lorsqu'une donnée reçoit la qualification de donnée à caractère personnel, son traitement doit respecter les règles édictées par le droit des données à caractère personnel. Ce régime, fondé sur la volonté de protéger les personnes contre les potentiels effets négatifs des traitements, organise un ensemble complexe de règles parmi lesquelles figure, en bonne place, la *confidentialité* des données[831]. Celle-ci se matérialise par une série de mesures devant être mises en place par les responsables du traitement et les sous-traitants pour assurer un niveau de sécurité adapté au risque[832]. Ces mesures de confidentialité visent notamment à atténuer les risques liés à la divulgation non autorisée de données à caractère personnel, tels que la destruction, la perte, l'altération ou l'accès non autorisé[833]. Ainsi, les données à caractère personnel, aussi anodines soient-elles, sont protégées par un principe de confidentialité, lequel empêche les tiers d'y accéder[834]. Ce principe restreint la communication de ces données aux *seules personnes autorisées*[835]. En établissant des catégories de personnes auxquelles les données peuvent être communiquées, le règlement européen entérine donc un principe de non-communicabilité des données à caractère personnel[836]. Seules quelques personnes, limitativement énumérées, peuvent accéder à ces données[837]. L'application de plus en plus large du principe de confidentialité aux données restreint donc *de facto* le champ des données pouvant circuler librement.

---

[831] Un principe d'interdiction de diffusion des données à caractère personnel est donc posé, v. not. B. Gauriau et A. Teissier, « Données personnelles et économiques : l'interdiction de diffuser », *JCP S* 2020, nº 20-21, p. 2028.
[832] Art. 32 § 1 du règlement UE nº 2016/679.
[833] Cons. 83 et art. 32 § 2 du règlement UE nº 2016/679.
[834] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nºs 1219 s., p. 559.
[835] Cons. 83 et art. 4 § 12 du règlement UE nº 2016/679. Sur les différentes catégories de tiers pouvant accéder aux données, v. *infra*, nº 426.
[836] Historiquement, l'objet du droit des données à caractère personnel était plutôt de protéger les données contre un accès ponctuel par des tiers. Comme le remarquait Monsieur Pascal Ancel, « les atteintes qui peuvent être sanctionnées sur le fondement de la loi Informatique et libertés étaient assez différentes de celles qui sont habituellement appréhendées à travers l'article 9 du code civil : celui-ci est surtout utilisé pour sanctionner des divulgations publiques de faits relatifs à la vie privée (…). Or ce ne sont pas de telles divulgations publiques qui sont à craindre dans le cas des fichiers : il s'agit surtout d'éviter que les informations rassemblées par le ficheur ne soient communiquées à un ou plusieurs tiers », P. Ancel, « La protection des données personnelles : aspects de droit privé français », *RID comp.* 1987, vol. 39, nº 3, p. 609, spéc. p. 617. Désormais, le droit des données personnelles sanctionne également des divulgations au grand public, notamment avec les obligations relatives aux violations de sécurité, prévues notamment à l'article 32 du règlement UE nº 2016/679
[837] Comme le rappelait Monsieur Ibrahim Coulibaly, « l'utilisation des données personnelles n'est admissible qu'au regard d'une activité ou d'une finalité venant légitimer le besoin d'accès aux données », ces données ne sont donc pas *librement* accessibles, v. I. Coulibaly, *La protection des données à caractère personnel dans le domaine de la recherche scientifique*, th. Grenoble, 2011, p. 33.

230. Les droits de la personne concernée comme limites à la circulation des données. Certaines des prérogatives reconnues aux personnes concernées leur permettent de restreindre encore davantage les données auxquelles les tiers peuvent accéder. En effet, le droit des données à caractère personnel leur reconnaît une variété de prérogatives à l'égard de leurs données[838]. Parmi ces prérogatives, le droit d'opposition et le droit à l'oubli peuvent avoir des effets sur les données auxquelles le public a le droit d'accéder. En ce qui concerne le droit d'opposition d'abord, celui-ci reconnaît à la personne concernée « le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant »[839]. Ce droit d'opposition peut être utilisé par les personnes concernées notamment pour s'opposer à la publication de données les concernant. Il est vrai que l'article 56 de la loi Informatique et libertés prévoit que « ce droit ne s'applique pas lorsque le traitement répond à une obligation légale ». Toutefois, sous l'empire de l'ancienne loi, le Conseil d'État avait considérablement réduit la portée de l'exception au droit d'opposition. En effet il avait affirmé que « le législateur, ainsi que le confirment d'ailleurs les travaux préparatoires, a entendu réserver la faculté de déroger au principe selon lequel toute personne physique a le droit de s'opposer, pour des motifs légitimes, à l'enregistrement de données à caractère personnel la concernant, aux seuls traitements automatisés de données autorisés par un acte réglementaire pris après avis de la CNIL en application des articles 26 et 27 de la loi du 6 janvier 1978 »[840]. Une telle lecture de la loi permet donc de reconnaître une application plus large du droit d'opposition des personnes concernées[841].

En pratique, plusieurs dispositions légales qui prévoient la publication de données reconnaissent également aux personnes concernées un droit d'opposition sur leurs données. C'est le cas notamment des données à caractère personnel contenues dans le registre du commerce et des sociétés[842], pour lesquelles les personnes physiques ont le droit de ne pas figurer dans le fichier mis à la disposition du public[843]. Ainsi,

---

[838] Pour un exposé sommaire de ces droits, v. C. Féral-Schuhl, *Cyberdroit 2020/2021,* 8e éd., Dalloz, 2020, nos 112.00 s.
[839] Art. 21 § 1 du règlement UE no 2016/679.
[840] CE Sec., 19 juill. 2010, *Fristot et Mme Charpy,* no 317182, *Lebon*, p. 320.
[841] Pour une analyse de cette décision sous l'angle du droit Informatique et libertés, v. A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, no 1544 s., p. 570 et M.-C. de Montecler, « Le Conseil d'État donne une leçon d'Informatique et libertés à l'Éducation nationale », *AJDA* 2010, p. 1454.
[842] La tenue de ce registre est prévue par l'article L. 123-1 du code de commerce. La communication de ces données est organisée par l'article R. 123-232 du code de commerce.
[843] Art. A. 123-96 du code de commerce.

dans certains cas, le droit d'opposition peut venir empiéter sur la liberté d'information et réduire la transparence pourtant souhaitée par le législateur[844].

En ce qui concerne le droit à l'oubli ensuite, son exercice peut également restreindre les informations accessibles au public. Si ce droit fera l'objet de développements plus conséquents dans la seconde partie de cette étude[845], il est d'ores et déjà possible de remarquer qu'en autorisant les personnes à demander l'effacement de données personnelles dont le traitement est pourtant licite[846], le législateur leur permet de morceler l'accès aux données les concernant. Il reconnaît ainsi aux personnes concernées le pouvoir d'empiéter sur la liberté d'information.

À ce titre, il est intéressant de remarquer que la Cour de justice de l'Union européenne n'hésite pas à affirmer que « les droits de la personne concernée protégés par les articles 7 et 8 de la Charte *prévalent*, *en règle générale*, sur la liberté d'information des internautes »[847]. L'intérêt individuel prévaut donc, par principe, sur l'intérêt collectif et une telle règle risque, à terme, de porter atteinte à la société dans son ensemble.

En augmentant le nombre de données entrant dans la notion de donnée à caractère personnel, on étend donc l'application de ces prérogatives. Pour autant, il est regrettable que les acteurs n'aient pas anticipé les effets de l'expansion de la notion sur la liberté d'information.

231. L'absence d'analyse des effets de l'expansion de la notion sur la liberté d'information. L'expansion de la notion s'est effectuée progressivement, naturellement et presqu'inéluctablement. Elle est principalement liée à une vision centrée autour de la protection des données personnelles et non autour de la protection de la personne[848]. C'est sans doute ce qui explique qu'aucune étude d'ampleur n'a été consacrée aux effets potentiels de cette expansion sur la liberté d'information[849]. Pourtant, dès 1980, l'OCDE rappelait que les règles relatives aux données devaient

---

[844] Le droit des données à caractère personnel peut donc être instrumentalisé par les personnes pour éviter de répondre à des obligations légales favorables à la transparence. Sur l'instrumentalisation de la protection des données à caractère personnel par les personnes morales, v. *supra,* n° 107.
[845] V. *infra*, n^os^ 411 s.
[846] N. Martial-Braz, « Le droit au déréférencement : vraie reconnaissance et faux-semblants ! », *Dalloz IP/IT* 2019, p. 631.
[847] CJUE, 24 sept. 2019, *Google LLC* c. *Commission nationale de l'informatique et des libertés,* C-507/17, § 66.
[848] Sur cette distinction, v. *supra*, n^os^ 10 s.
[849] Madame Éloïse Gratton consacre tout de même des développements conséquents à cette analyse, v. É. Gratton, *Redefining personal information in the context of the Internet*, th. Paris II et Montréal, 2012, p. 72 s.

concilier le droit au respect de la vie privée et la libre circulation de l'information[850]. Si le législateur européen oblige les États membres à concilier la protection des données et la liberté d'information[851], rien dans la loi française n'organise une telle mise en balance. En effet, la loi Informatique et libertés ne prévoit aucune disposition particulière pour articuler la mise en œuvre du droit des données à caractère personnel avec la liberté d'information. Un tel mutisme témoigne de l'intérêt relatif accordé par les acteurs du droit des données à caractère personnel aux effets de l'expansion de la notion sur les autres libertés[852].

232. L'influence de l'expansion de la notion de donnée à caractère personnel : la diminution des informations pouvant circuler librement. La qualification de plus en plus automatique des données en données à caractère personnel revient, *de facto*, à appliquer le principe de non-communication à un nombre croissant de données. L'expansion de la notion de donnée à caractère personnel restreint donc les informations pouvant circuler *librement* et atteint le droit de « chercher, recevoir et répandre » des informations.

Comme l'expliquait déjà William Prosser au sujet de la protection de la *privacy,* « pour déterminer où tracer la ligne de protection, les juridictions ont été invitées à exercer rien d'autre qu'un pouvoir de *censure* à l'égard de ce que le public peut lire »[853]. Cette remarque est parfaitement transposable à la protection des données à caractère personnel, puisqu'une fois qualifiées comme telles, les données ne peuvent plus circuler librement. En augmentant le domaine de la donnée à caractère personnel, on empêche le public d'avoir accès à un nombre croissant de données et on censure les informations auxquelles il peut accéder[854]. L'expansion de la notion remet donc en

---

[850] OCDE, Lignes directrices du 23 sept. 1980 sur la vie privée et les flux transfrontières de données à caractère personnel.
[851] Art. 85 du règlement UE nº 2016/679.
[852] L'article 80 de la loi nº 78-17 du 6 janvier 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018 traite uniquement de la liberté d'expression et se limite à l'expression universitaire, artistique ou littéraire et à l'exercice, à titre professionnel, de l'activité de journaliste, v. *infra,* nº 240. Pour Monsieur Pierre Trudel, l'impératif de libre circulation des informations « est habituellement oublié par plusieurs auteurs et groupes de pression s'intéressant à la protection des renseignements personnels », P. Trudel, « La protection de la vie privée dans les systèmes d'information relatifs à la santé. Ajuster les concepts aux réalités des réseaux », in *Les pratiques de recherche biomédicales visitées par la bioéthique*, dir. C. Hervé, B.-M. Knoppers et P. Molinari, Dalloz, 2003, p. 165.
[853] W. Prosser, « Privacy », *California Law Review* 1960, vol. 48, p. 383 s. [48 CAL. L. REV. 383], spéc. p. 413.
[854] D'ailleurs, pour Madame Frédérique Brocal von Plauen, le droit à la vie privée est parfois « trop bien protégé puisque sous prétexte d'atteinte à la vie privée, certaines décisions se transforment en censure, rendant impossible toute publication », F. Brocal von Plauen, *Le droit à l'information en France*, th. Lyon II, 2004, p. 256.

cause le délicat équilibre entre la protection des données personnelles et la libre circulation de l'information.

233. Exemples des effets de l'expansion de la notion sur la liberté d'information. Plusieurs exemples illustrent les effets négatifs provoqués par l'expansion de la notion sur la circulation d'informations. La qualification d'un arbre remarquable comme donnée à caractère personnel est une première illustration de ces effets. Considérer qu'un arbre remarquable est une donnée à caractère personnel revient en pratique à interdire aux individus de recevoir et disséminer librement des informations concernant ces arbres. Ainsi, les études dédiées à ce sujet seront soumises aux règles du droit des données à caractère personnel, lesquelles permettent notamment aux personnes concernées (c'est-à-dire celles sur la propriété desquelles un tel arbre se situe) de s'y opposer. Pourtant, un tel rattachement entre l'arbre et la personne est le fait d'un traitement particulier visant précisément à obtenir des informations sur la personne. L'expansion sans limite de la notion de donnée à caractère personnel restreint donc la capacité des individus à accéder librement aux données. Comme l'expliquait déjà en 1994 Monsieur Xavier Agostinelli au sujet de l'extension du droit au respect de la vie privée, « déviée à l'usage, de sa finalité première, une telle revendication systématique sur le fondement de l'article 9 du code civil ne pouvait déboucher que sur de nombreux abus, tout en laissant planer le risque d'aboutir à une négation pure et simple du droit à l'information »[855]. Cette négation du droit à l'information risque de porter atteinte à la protection des personnes. L'expansion de la notion de donnée à caractère personnel touche donc bel et bien à l'effectivité de la protection des personnes.

234. La liberté d'information nécessaire au développement libre de la personnalité. Les libertés liées à l'information interagissent les unes avec les autres et s'enrichissent mutuellement : liberté d'expression, liberté d'information, liberté d'opinion entretiennent donc d'importants rapports[856]. La liberté d'information entretient également des rapports avec le droit au respect de la vie privée.

[855] X. Agostinelli, *Le droit à l'information face à la protection civile de la vie privée*, th. Aix-en-Provence, 1994, Librairie de l'Université d'Aix-en-Provence, n° 36, p. 33.
[856] S. Hennette-Vauchez et D. Roman, *Droits de l'Homme et libertés fondamentales*, 4e éd., Dalloz, 2020, n° 493, p. 370.

Classiquement, les juristes les opposent[857] et considèrent que des collisions sont à craindre[858].

En matière de données à caractère personnel, la confrontation entre ces deux matières apparaît moins conflictuelle. En effet, étant donné que les informations inclues dans la notion de donnée à caractère personnel peuvent être indirectement identifiantes, voire très indirectement identifiantes, ces données touchent moins personnellement les individus. Seuls les traitements tendant à rétablir un lien entre la donnée et la personne permettent de renseigner sur les personnes. D'ailleurs, l'atteinte à la personne résultant d'une diffusion de données telles que des adresses IP, des arbres remarquables ou des données géographiques est bien moins importante que celle résultant de traitements portant atteinte à la vie privée.

En dehors de ces traitements particuliers qui peuvent être liées aux personnes, ces données restent très utiles pour l'élaboration de statistiques ou d'études. Restreindre leur circulation a donc tendance à brider la capacité des personnes à s'informer librement sur ces sujets et à développer leur propre opinion[859]. Dès lors, en permettant aux informations de circuler, on permet aux personnes de développer librement leur personnalité. Une telle faculté participe sans conteste à une meilleure effectivité de la protection des personnes.

235. L'expansion de la notion de donnée à caractère personnel, un facteur parmi d'autres. L'expansion du domaine des données à caractère personnel est loin d'être le seul élément ayant un impact négatif sur la liberté d'information. Si un règlement européen de 2018 a consacré le principe de libre circulation des données non personnelles[860], d'autres régimes spéciaux et exceptions rongent de plus en plus le principe de la liberté d'information. À titre d'exemple, le secret des affaires[861], le secret

---

[857] X. Agostinelli, *Le droit à l'information face à la protection civile de la vie privée*, th. Aix-en-Provence, 1994, Librairie de l'Université d'Aix-en-Provence, nº 11, p. 20 ; D. Chauvet, *La vie privée. Étude de droit privé,* th. Paris-Sud, 2014, nº 576, p. 444.

[858] B. Teyssié, *Droit des personnes*, 21e éd., LexisNexis, 2019, nº 160, p. 151.

[859] Pour des développements sur l'interaction entre le besoin d'information et la liberté d'autodétermination, v. *infra*, nº 416.

[860] Règlement UE nº 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, *JOUE* 28 nov. 2018, L-303/65, p. 65 s.

[861] Le secret des affaires protège très largement les informations qui revêtent « une valeur commerciale, effective ou potentielle », v. directive UE nº 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulguées (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, *JOUE* 15 juin 2016, L-157/1, p. 1 s., transposée en droit français par la loi nº 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires, *JORF* 31 juill. 2018, nº 0174, texte 1. Sur les interactions entre le secret des affaires et la liberté d'informer, v. not. M. Vaudano, « Secret des affaires : le texte adopté par le Parlement menace-t-il la liberté d'informer ? », *Le Monde* 27 févr. 2018.

des délibérations du Gouvernement, les documents classifiés[862] ou la propriété intellectuelle[863] constituent d'autres limites à cette liberté[864]. Face à ces assauts, la substance de la liberté d'information se réduit inexorablement au risque de devenir, peut-être un jour, une peau de chagrin[865].

§ II. Les effets sur la liberté d'expression

236. Plan. La liberté d'expression est dotée d'un puissant pouvoir évocateur[866]. Décrite comme l'un des droits les plus précieux de l'homme[867], elle est un droit hors du commun[868]. Son exercice est la marque de la vitalité d'une démocratie[869], notamment parce qu'aucun régime qui ne reconnaîtrait ni n'imposerait les libertés d'opinion et d'expression ne pourrait se réclamer de la liberté[870]. La liberté d'expression appartient historiquement aux droits de l'homme et est protégée par les sources juridiques les plus élevées (A). Pour autant, selon certains auteurs, elle menacerait le respect de l'individualité de chacun[871], notamment parce qu'elle poursuit l'objectif de communiquer au public toutes les informations qu'il est en droit de connaître[872]. Cette liberté entretient donc des rapports complexes avec le droit des données à caractère personnel (B).

---

[862] Par exemple, sur les secrets restreignant la communication des documents administratifs, v. art. L. 311-5 du code des relations entre le public et l'administration. Sur les limites à cette ouverture, v. L. Cluzel-Métayer, « Les limites de l'open data », *AJDA* 2016, p. 102.

[863] Sur les potentiels effets néfastes de la propriété intellectuelle sur l'innovation, v. L. Lessig, *The future of ideas : the fate of the commons in a connected world,* Random House, 2001.

[864] V. par ex., A. Pezard, « Les limites à la protection – vers une nouvelle proportionnalité judiciaire », *Propriété Industrielle* 2018, nº 9, dossier 12. Pour Monsieur Éric Alt, vice-président de l'association Anticor, « les journalistes et les lanceurs d'alerte se retrouveront toujours en position de défense pour démontrer au juge que la divulgation des faits a un intérêt général. S'ils n'y arrivent pas, cela leur coûtera très cher. Ils auront toujours une épée de Damoclès au-dessus de la tête. Le secret devient la règle et la transparence l'exception », A. Poussart, « Loi sur le secret des affaires : une épée de Damoclès pour les lanceurs d'alerte et les journalistes ? », *Public Sénat* 16 avr. 2018.

[865] Dans le roman de Balzac, le jeune Raphaël de Valentin, désabusé par ses pertes aux jeux, accepte un pacte diabolique avec un peau magique. Celle-ci a le pouvoir d'exaucer ses vœux, mais chaque désir exaucé fait diminuer la taille de la peau, symbole de la vie de son propriétaire. Telle une peau de chagrin, la liberté d'information se réduit devant les vœux de protection des données personnelles les plus larges.

[866] G. Lécuyer, *Liberté d'expression et responsabilité. Étude de droit privé,* th. Paris I, 2004, Dalloz, nº 17, p. 29.

[867] Art. 11 de la Déclaration des droits de l'homme et du citoyen.

[868] F. Sudre (dir.), *Droit européen et international des droits de l'homme*, 14e éd., PUF, 2019, nº 537, p. 807.

[869] H. Oberdorff, *Droits de l'homme et libertés fondamentales,* 7e éd., LGDJ, 2019, nº 463, p. 600. D'ailleurs, la CEDH rappelle régulièrement que « la liberté d'expression constitue l'un des fondements essentiels d'une société démocratique et l'une des conditions primordiales de son progrès et de l'épanouissement de chacun », CEDH, 17 juill. 2001, *Association Ekin* c. *France*, nº 39288/98, § 56. Le Conseil constitutionnel considère aussi que « la liberté d'expression et de communication est d'autant plus précieuse que son exercice est une condition de la démocratie et l'une des garanties du respect des autres droits et libertés ; que les atteintes portées à l'exercice de cette liberté doivent être nécessaires, adaptées et proportionnées à l'objectif d'intérêt général poursuivi », Cons. const., 20 mai 2011, nº 2011-131 QPC, cons. 7 ; Cons. const., 10 juin 2009, nº 2009-580 DC, cons. 15.

[870] J. Baechler, « Les libertés d'opinion et d'expression », *RDP* 2015, nº 2, p. 308.

[871] G. Lécuyer, *Liberté d'expression et responsabilité. Étude de droit privé,* th. Paris I, 2004, Dalloz, nº 56, p. 79.

[872] D. Chauvet, *La vie privée. Étude de droit privé,* th. Paris-Sud, 2014, nº 569, p. 439.

A. La protection de la liberté d'expression

237. La liberté d'expression, un droit fondamental. Nombreux sont les textes qui garantissent, aux niveaux national et international, la liberté d'expression. Ainsi, en vertu de l'article 11 de la Déclaration des droits de l'homme et du citoyen, « la libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme : tout Citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la Loi ». L'article 11 de la Charte des droits fondamentaux de l'Union européenne et l'article 10-1 de la CESDH la protègent également en garantissant son *aspect transfrontière*[873]. Avec le développement du numérique et particulièrement d'Internet, cette dimension transnationale de la liberté d'expression a pris un nouvel essor.

238. Le numérique et Internet amplifient la liberté d'expression. Les évolutions intervenues dans le domaine des technologies de l'information et de la communication ont généré des changements sociétaux considérables[874]. En facilitant l'accès aux contenus et en libérant les capacités de diffusion, Internet permet une circulation mondiale de l'information. La liberté d'expression a alors pu conquérir de nouveaux espaces et son exercice s'est démocratisé[875]. Historiquement, seule une minorité de personnes (le plus souvent les artistes et les journalistes) exerçait cette liberté et plutôt à un niveau local. Les divers outils d'édition et de publication, tels que les blogs, les sites Internet ou les forums de discussion, ont facilité l'exercice de la liberté d'expression d'un plus grand nombre de personnes[876]. D'ailleurs, la CEDH a affirmé que « grâce à leur accessibilité ainsi qu'à leur capacité à conserver et à diffuser de grandes quantités de données, les sites Internet contribuent grandement à améliorer l'accès du public à l'actualité et, de manière générale, à faciliter la communication de l'information »[877]. Internet permet donc aux personnes de s'exprimer plus facilement

---

[873] F. Sudre (dir.), *Droit européen et international des droits de l'homme*, 14e éd., PUF, 2019, no 540, p. 813. Ce caractère transfrontière a été mis en évidence dans plusieurs affaires, v. not. CEDH, 28 mars 1990, *Groppera Radio AG et autres* c. *Suisse*, no 10890/84, § 55 et CEDH, 22 mai 1990, *Autronic AG* c. *Suisse*, no 12726/87, § 52.
[874] H. Oberdorff, *Droits de l'homme et libertés fondamentales,* 7e éd., LGDJ, 2019, no 301, p. 408.
[875] V. par ex. le rôle d'Internet dans les printemps arabes, V. Morin, « Comment Internet a fait les "printemps arabes" », *Le Monde* 24 oct. 2017. V. aussi. Z. Tüfekçi, *Twitter and tear gas: the power and fragility of networked protest,* Yale University Press, 2017.
[876] M. Zwolinska, *Sécurité et libertés fondamentales des communications électroniques en droit français, européen et international*, th. Nice, 2015, nos 78 s., p. 80 s. ; H. Oberdorff, *Droits de l'homme et libertés fondamentales,* 7e éd., LGDJ, 2019, no 305, p. 413.
[877] CEDH, 10 mars 2009, *Times Newspapers Ltd* c. *Royaume-Uni*, no 3002/03 et no 23676/03, § 27. La Cour a confirmé à plusieurs reprises que « Internet est aujourd'hui devenu l'un des principaux moyens d'exercice par les individus de leur droit à la liberté de recevoir ou de communiquer des informations ou des idées », et « la

et de partager, en un clic, des données à travers le monde. Cette capacité facilite la diffusion d'informations, y compris personnelles. C'est pourquoi la liberté d'expression entretient des rapports parfois compliqués avec la protection des données à caractère personnel.

B. Les rapports entre la liberté d'information et le droit des données à caractère personnel

239. L'absence d'analyse des effets de l'expansion de la notion de donnée à caractère personnel sur la liberté d'expression. Le principe selon lequel la liberté d'expression rencontre des limites est généralement admis[878]. La question de la nature exacte de ces limites est plus complexe dès lors qu'elle dépend de la casuistique. Le droit a justement mis en place des mécanismes pour garantir un équilibre entre les différents intérêts en présence[879]. Ainsi, l'article 85 du règlement européen 2016/679 prévoit qu'une conciliation doit être opérée, par les législations des États membres, entre le droit à la protection des données à caractère personnel et le droit à la liberté d'expression. Le législateur français a prévu une articulation réduite. En effet, l'article 80 de la loi Informatique et libertés a organisé un système dérogatoire au droit des données à caractère personnel pour la liberté d'expression. Toutefois, le législateur français a retenu une conception très stricte de la liberté d'expression. En effet, là où l'article 85 du règlement européen prévoit que la protection des données à caractère personnel doit être conciliée avec la liberté d'expression, la loi française vise uniquement les traitements de données à caractère personnel « aux fins de journalisme et d'expression littéraire et artistique »[880]. Plus particulièrement, ce régime se limite aux traitements de données à des fins journalistiques *à titre professionnel*, d'expression universitaire, artistique ou littéraire.

---

possibilité pour les individus de s'exprimer sur Internet constitue un outil sans précédent d'exercice de la liberté d'expression », CEDH, 1er déc. 2015, *Cengiz et autres* c. *Turquie*, nº 48226/10 et nº 14027/11, § 49 et 52.

[878] S. Hennette-Vauchez et D. Roman, *Droits de l'Homme et libertés fondamentales*, 4e éd., Dalloz, 2020, nº 502, p. 373.

[879] F. Sudre, « Le contrôle de proportionnalité de la Cour européenne des droits de l'homme. De quoi est-il question ? », *JCP G* 2017, nº 11, doctr. 289, § 3.

[880] La loi française est donc plus réductrice que le droit européen. Plus précisément, l'article 80 de la loi nº 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018 retient une acception réduite de la liberté d'expression puisque le bénéfice de cette disposition est réservé aux seuls journalistes exerçant cette activité « à titre professionnel ». Une telle conception va à l'encontre de celle retenue notamment par la Cour de justice de l'Union européenne qui définit les activités de journalisme largement. Ces activités sont considérées comme « celles qui ont pour finalité la divulgation au public d'informations, d'opinions ou d'idées, sous quelque moyen que ce soit » et incluent également les activités non professionnelles, CJUE, 14 févr. 2019, *Sergejs Buivids*, C-345/17, § 53 s. Pour un commentaire de cette décision, v. A. Debet, « Une vidéo publiée sur YouTube est un traitement de données à des fins de journalisme », *CCE* 2019, nº 4, comm. 27. Pour une étude de cette question, v. A. Debet, « Traitement de données aux fins de journalisme : état des lieux et perspectives », *Légipresse* 2020, hors-série nº 63, p. 51.

Par ailleurs, rien dans la lettre du texte ou dans les débats législatifs ne montre une prise en considération des effets de l'expansion de la notion de donnée à caractère personnel sur la liberté d'expression[881].

240. Une mise en œuvre délicate du principe de proportionnalité. En principe, ce sont les juridictions qui assurent des contrôles de proportionnalité pour réaliser le « juste équilibre entre les différents intérêts en présence »[882]. Pendant longtemps, la mise en balance entre les intérêts opposait des informations protégées au titre de la vie privée (entretenant donc un lien fort avec la personne) et la liberté d'information ou la liberté d'expression[883]. Avec la fondamentalisation du droit des données à caractère personnel, des informations indirectement identifiantes peuvent désormais être mises en balance avec d'autres libertés[884]. De tels contrôles de proportionnalité ont-ils encore un sens lorsque l'un des éléments « mis en balance » est une information dont le rattachement avec la personne est très indirect ? En effet, une information telle qu'une simple adresse IP ou un arbre remarquable peut-elle légitimement venir restreindre l'exercice d'une liberté fondamentale telle que la liberté d'expression ? Il semble assez évident que ces informations, prises en tant que telles, ne devraient pas recevoir une protection aussi forte que celle applicable aux données dont le lien avec la personne est certain et direct. D'ailleurs, la Cour de cassation n'hésite pas, lorsque la liberté d'expression est en jeu, à censurer les juges du fond ayant retenu une atteinte à la vie privée lorsque les informations sur la personne étaient anodines[885].

Ainsi, lorsque la donnée est trop éloignée de la personne, elle ne devrait pas pouvoir restreindre l'exercice de la liberté d'expression. Pourtant, c'est bien le résultat inverse qui est atteint avec l'expansion continue de la notion de donnée à caractère personnel et la fondamentalisation de ce droit[886].

---

[881] Les autres acteurs de la protection des données à caractère personnel, tels que la CNIL (dont le rôle était initialement le développement d'une informatique respectueuse des libertés), ne se sont pas non plus intéressés aux éventuels effets négatifs d'une telle expansion.
[882] CEDH, 13 août 1981, *Young, James et Webster* c. *Royaume-Uni*, n° 7601/76 et n° 78066/77, § 65.
[883] D'ailleurs, « lorsque la révélation d'une information sur une personne met en cause un événement d'actualité et donc la liberté de l'information ou encore que cette information est anodine, le juge en déduit que le droit subjectif au respect de la vie privée n'est pas en cause », X. Dupré de Boulois, « Regard extérieur sur une jurisprudence en procès », *JCP G* 2016, n° 18, doctr. 552, § 10.
[884] V. *supra*, n° 221.
[885] Cass. civ. 2e, 8 juill. 2004, n° 02-17.458, *Bull. civ.* 2004, II, n° 388, p. 326.
[886] D'ailleurs, selon une opinion doctrinale, « tout type de données peut être englobé car la définition repose sur le postulat qu'il n'y a pas de données anodines », v. A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, n° 496, p. 220.

241. La liberté d'expression encadrée par la présence de données à caractère personnel. En réduisant les informations pouvant circuler librement, le risque est de réduire les capacités d'expression sur certains sujets[887]. Dans le documentaire *Ouvrir la Voix*, Madame Amandine Gay évoque subtilement la difficulté de débattre publiquement de sujets pour lesquels le traitement des informations nécessaires au débat est fortement encadré[888]. Ce documentaire sur les femmes noires d'Europe met notamment en lumière le sujet des discriminations existant à leur égard. La question de ces discriminations fait l'objet de nombreux tabous, et les statistiques qui y sont liées, notamment celles sur l'emploi, n'existent pratiquement pas car le traitement de ces données est fortement encadré[889]. En effet, les restrictions imposées sur les traitements de données relatives à l'ethnie d'une personne[890] – définie comme donnée sensible[891] – rendent plus difficile de quantifier statistiquement d'éventuels phénomènes[892]. Sur cette question, deux courants s'opposent[893]. D'un côté, les opposants à l'élaboration de ce type de statistiques qui fragiliseraient la cohésion sociale et la culture universaliste à la française[894]. De l'autre, les partisans de leur élaboration car elles seraient avant tout un outil de connaissance essentiel pour mesurer l'étendue des discriminations[895].

Cette question de l'existence des statistiques ethniques illustre celle plus profonde des effets de l'expansion de la notion de donnée à caractère personnel sur les capacités d'expression. En reconnaissant à une donnée la qualification de donnée à caractère personnel, on restreint le pouvoir d'expression des autres personnes sur cette

---

[887] Sur cette théorie v. not. les développements de E. Morozov, « The real privacy problem », *MIT Tech Review* 2013, vol. 116, p. 32.
[888] A. Gay, *Ouvrir la voix*, Bras de Fer Production et Distribution, 2017.
[889] Art. 9 du règlement UE nº 2016/679 interdit notamment le traitement des informations relatives à l'ethnie d'une personne.
[890] Dans une décision médiatisée, le Conseil constitutionnel s'est prononcé sur les études relatives à la mesure de la diversité. Après avoir déclaré que l'article permettant la réalisation de ces traitements était un « cavalier législatif », c'est-à-dire qu'il était « dénué de tout lien avec les dispositions qui figuraient dans le projet de loi initial », le Conseil constitutionnel a considéré que « si les traitements nécessaires à la conduite d'études sur la mesure de la diversité des origines des personnes, de la discrimination et de l'intégration peuvent porter sur des données objectives, ils ne sauraient, sans méconnaître le principe énoncé par l'article 1er de la Constitution, reposer sur l'origine ethnique ou la race », Cons. const., 15 nov. 2007, nº 2007-557 DC, cons. 29. Sur cette question, v. A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nos 890 s., p. 356 s.
[891] Art. 9 § 1 du règlement UE nº 2016/679.
[892] Récemment, l'INSEE a rappelé qu'elle établissait des statistiques ethniques publiques, tout en rappelant que celles-ci demeurent strictement encadrées, v. S. Le Minez, « Oui, la statistique publique produit des statistiques ethniques. Panorama d'une pratique ancienne, encadrée et évolutive », *Blog Insee* 31 juill. 2020.
[893] F. Héran, « France/États-Unis : deux visions de la statistique des origines et des minorités ethniques », *Santé, Société et Solidarité* 2005, nº 1, p. 167.
[894] Pour une étude sur l'universalisme français, v. L. Béru, « Statistiques ethniques, débats sociétaux et études en communication. L'universalisme français à la lumière du différentialisme anglo-saxon », *Médiation & Information* 2008, nº 28, p. 53.
[895] G. Dagorn, « La difficile utilisation des statistiques ethniques en France », *Le Monde* 19 mars 2019 ; v. aussi, M. Wanga, L-G. Tin et H. Le Bras, « Faut-il des statistiques ethniques ? », *Binge Audio* mai 2019

donnée. L'extension du domaine de la donnée à caractère personnel réduit donc *de facto* celui de la liberté d'expression.

242. Exemples de l'effet inhibiteur de la protection des données à caractère personnel sur la liberté d'expression. L'expansion de la notion associée aux sanctions dissuasives[896] invite les responsables du traitement à appliquer un véritable *principe de précaution* lorsqu'ils traitent des données. Plusieurs exemples illustrent les risques d'inhibition sur la recherche ou la liberté d'expression provoqués par la protection des données à caractère personnel.

Les conséquences liées à l'étude menée par l'organisation EU Disinfo Lab en sont une première illustration. À l'occasion de « l'affaire Benalla », l'organisation avait analysé les réactions sur le réseau social Twitter afin d'identifier l'éventuelle présence d'une ingérence étrangère. Pour répondre aux critiques sur leurs méthodes, les auteurs de l'étude avaient publié les fichiers de données utilisés pour la réaliser[897]. L'un de ces fichiers classait les comptes Twitter en fonction de leur prétendue appartenance politique. Cette publication avait provoqué un véritable tollé[898], alors même que cette étude avait un objectif de recherche[899] et que les données utilisées sont accessibles à tous[900]. Monsieur Nicolas Vanderbiest, l'un des principaux auteurs de cette étude, a subi des menaces d'une telle nature qu'il s'est senti obligé de cesser ses activités universitaires[901]. Les menaces fondées sur le droit des données à caractère personnel ont donc des effets sur la capacité des personnes à s'exprimer.

Un autre exemple de l'effet inhibiteur est celui de Monsieur Nathann Cohen, créateur du moteur de recherche Steinertriples, lequel facilite l'accès aux nominations publiées dans le Journal officiel[902]. La publication de ces nominations au Journal officiel répond à un objectif d'intérêt général fondé sur le besoin du public d'avoir accès à ces informations. Reprenant ces informations, le moteur de recherche rend l'information publique plus accessible en permettant à toute personne de trouver

---

[896] L'article 85 du règlement UE nº 2016/679 prévoit que les sanctions doivent être « effectives, proportionnées et dissuasives ».
[897] EU Disinfo Lab avait fourni le 8 août 2018 un lien vers ces deux fichiers.
[898] Le nombre de plaintes auprès de la CNIL a été si important que celle-ci s'est saisie du dossier, v. not. CNIL, « Étude réalisée à partir de messages postés sur Twitter : la CNIL est saisie du dossier », 9 août 2018. L'instruction des plaintes est effectuée en coordination avec son homologue belge.
[899] Calimaq, « Affaire DisinfoLab : quelles retombées potentielles sur la recherche publique et la science ouverte ? », *S.I.Lex* 21 août 2018.
[900] Ces données étaient issues de l'interface de programmation d'application (également dénommée *API*) du site Twitter.
[901] N. Vanderbiest, « Bonjour à tous », *Medium* 10 août 2018.
[902] Le site Steinertriples facilite les recherches liées aux nominations publiées dans le Journal officiel.

facilement une nomination. En cela, ce moteur de recherche participe à l'intérêt public et à l'information du public. Pourtant, Monsieur Cohen reçoit régulièrement des demandes d'effacement et d'opposition au traitement ou des menaces de poursuites des personnes concernées par ces nominations. Dans l'incertitude des conditions de légalité de son traitement, Monsieur Cohen a hésité à mettre fin à son projet.

Ces exemples montrent à quel point la protection des données à caractère personnel peut avoir des effets inhibiteurs sur la liberté d'expression. En dehors du contentieux judiciaire[903], l'équilibre entre ces deux droits est donc plutôt favorable à la protection des données, notamment en raison des risques liés aux sanctions et à leur effet dissuasif pour les plus petits acteurs[904]. L'expansion de la notion de donnée à caractère personnel amplifie encore davantage ces risques.

243. Conclusion de chapitre. L'expansion de la notion de donnée à caractère personnel a des effets sur les autres droits et libertés[905]. Les effets de cette expansion sont très relatifs à l'égard de la protection de la vie privée. Celle-ci a même tendance à être contre-productive. D'une part, elle place sur un pied d'égalité les atteintes potentielles et les atteintes effectives à la personne. D'autre part, elle donne une illusion de protection, sans pour autant apporter les garanties nécessaires à une défense efficace des données[906]. À cela s'ajoutent également des effets négatifs sur les libertés pour lesquelles le traitement d'informations est essentiel. Naturellement, l'augmentation du domaine de la donnée à caractère personnel réduit celui des libertés d'information et d'expression. Ces effets ne semblent pas justifiés, notamment parce que les informations sont parfois très éloignées des personnes[907]. Finalement, cette expansion

---

[903] Selon une opinion doctrinale majoritaire, et après une analyse jurisprudentielle, la vie privée céderait souvent au profit de la liberté d'expression, v. par ex. D. Mazeaud, « Vie privée des personnes publiques : toujours moins ? », *RTD civ.* 2018, p. 362.

[904] Sur les effets négatifs du règlement européen sur la liberté d'expression, v. R. Layton, « The 10 problems of GDPR. The US can learn from the EU's mistakes and leapfrog its policy », audition devant le Sénat américain, *American Enterprise Institute* 12 mars 2019, p. 5 s.

[905] La plupart des évolutions de cette matière semble avoir été conduite au seul prisme de la protection des données à caractère personnel et ont tendance à minimiser les effets de l'expansion sur les autres libertés. La même remarque peut aussi être formulée à l'égard des négociations du règlement européen sur la protection des données : les négociateurs de ce texte (au sein de la Commission européenne mais aussi au sein des ministères ayant déterminé la position des États membres) étaient plutôt des spécialistes de la protection des données à caractère personnel que des spécialistes des libertés sur Internet.

[906] P. Trudel, « La protection de la vie privée dans les systèmes d'information relatifs à la santé. Ajuster les concepts aux réalités des réseaux », in *Les pratiques de recherche biomédicale visitées par la bioéthique*, dir. C. Hervé, B.-M. Knoppers et P. Molinari, Dalloz, 2003, p. 168.

[907] D'ailleurs Monsieur Pierre Trudel considérait dès 2003 que « l'on se retrouve avec des législations imposant toujours plus de restrictions à la circulation des informations portant sur les personnes, sans pour autant procurer une protection effective à la vie privée de ces dernières », P. Trudel, « La protection de la vie privée dans les systèmes d'information relatifs à la santé. Ajuster les concepts aux réalités des réseaux », in *Les pratiques de*

ne sert pas les objectifs de protection des personnes, et une nouvelle notion de donnée à caractère personnel doit donc être proposée.

recherche biomédicales visitées par la bioéthique, dir. C. Hervé, B.-M. Knoppers et P. Molinari, Dalloz, 2003, p. 165.

Chapitre II – Les propositions d'encadrement de la notion de donnée à caractère personnel

244. Le besoin d'apporter des limites à la notion. Le constat de l'expansion de la notion et celui de ses effets illustre bien le fameux proverbe « qui trop embrasse mal étreint »[908]. Contrairement à une opinion doctrinale dominante qui voit dans cette expansion un gage de meilleure protection des personnes, nous considérons que celle-ci présente des effets collatéraux, souvent sous-estimés. Face aux risques d'une expansion potentiellement sans limite de la notion de donnée à caractère personnel, il convient de reconnaître que celle-ci a besoin d'être encadrée afin d'éviter qu'elle ne s'applique trop largement[909]. La recherche d'un équilibre entre l'inclusion dans la notion de donnée à caractère personnel d'informations liées aux personnes tout en assurant l'exclusion des informations éloignées des personnes semble périlleuse. Comment circonscrire l'application de la notion sans pour autant fragmenter la protection résultant du droit des données personnelles ?

245. Des propositions doctrinales. L'examen des travaux doctrinaux montre que le constat du besoin de renouvellement notionnel est partagé[910]. Partant du constat de la difficulté de protéger les personnes contre la captation de leurs données, ces travaux ont proposé de nouvelles définitions de la donnée à caractère personnel[911]. Ils offrent d'intéressants points de vue et proposent des analyses pertinentes des dynamiques engendrées par les développements numériques. Pour autant, répondent-ils à toutes les

---

[908] Cette formule figurait déjà dans le discours du député Jean Foyer qui avait proclamé qu'il convient « dans une matière aussi neuve, de se souvenir du proverbe : "Qui trop embrasse mal étreint". C'est pourquoi le projet prévoit que les dispositions légales s'appliqueront seulement aux traitements automatisés d'informations nominatives, les seules qui soient vraiment dangereuses pour la vie privée et pour les droits individuels des citoyens », v. J. Foyer, 1re séance du mardi 4 oct. 1977, *JORF AN* 5 oct. 1977, nº 79, p. 5783. Dans cette même idée, Jean Rivero parlait du risque de « filtrer le moustique et de laisser passer le chameau », J. Rivero, « À propos de la loi Sécurité et liberté : filtrer le moustique et laisser passer le chameau. À propos de la décision du Conseil constitutionnel du 20 juin 1981 », *AJDA* 1981, p. 275.

[909] H. Guillard, « Critique du Web² (3/4) : Toutes les données sont devenues personnelles », *Internetactu.net* 21 sept. 2009.

[910] Pour une analyse synthétique des critiques et options avancées, v. O. Tambou, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, nºs 78 s., p. 71 s. ; N. Purtova, « The law of everyhting. Broad concept of personal data and future of EU data protection law », *Law, Innovation and Technology* 2018, nº 10, p. 1.

[911] V. not. P.-Y. Marot, *Les données et informations à caractère personnel. Essai sur la notion et ses fonctions,* th. Nancy, 2007 ; É. Gratton, *Redefining personal information in the context of the Internet*, th. Paris II et Montréal, 2012 ; J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon et S. Alliot, *Essai de qualification de la notion de données à caractère personnel,* th. Besançon, 2018.

difficultés identifiées ? Dans le cas où ces propositions n'y parviennent pas, il conviendra de proposer une nouvelle approche.

246. Plan. Plusieurs juristes ont proposé des critères pour renouveler la notion de donnée à caractère personnel. À l'étude, ces propositions se révèlent insatisfaisantes et ne répondent pas aux problèmes identifiés (Section I). Nous proposerons donc une approche nouvelle fondée sur un critère téléologique (Section II).

SECTION I – LE CARACTÈRE INSATISFAISANT DES PROPOSITIONS DOCTRINALES EXISTANTES

247. Les propositions de nouvelles définitions. La question de la pertinence et de l'efficacité du droit des données à caractère personnel est ancienne[912]. Sa réponse doit d'ailleurs sans cesse être mise à jour du fait de l'évolution des technologies et des nouvelles formes d'atteinte que celles-ci permettent. Les réponses juridiques se doivent donc d'être effectives et renouvelées. C'est dans cet objectif que la doctrine juridique a proposé des ajustements pour garantir l'adéquation de la protection juridique aux évolutions techniques.

248. Plan. Parmi ces propositions, trois d'entre elles recommandent d'adopter de nouveaux critères pour définir la notion de donnée à caractère personnel. Une opinion doctrinale fonde l'application de la notion sur le risque de dommage (§ I) ; une autre s'oriente autour d'un critère de contrôle (§ II) ; et la troisième propose de retenir une analyse contextuelle (§ III).

§ I. L'approche fondée sur le dommage

249. Présentation. Madame Éloïse Gratton a proposé, dans une thèse de 2012, de redéfinir la notion de donnée personnelle dans le contexte d'Internet[913]. Selon elle, la notion de donnée personnelle est à la fois trop large et trop restrictive pour répondre au

[912] Déjà en 1997, la CEDH affirmait l'importance pour les droits internes de prévoir des garanties aptes à protéger efficacement les données à caractère personnel, CEDH, 4 déc. 2008, *S. et Marper* c. *Royaume-Uni*, n° 30562/04 et n° 30566/04, § 103.
[913] É. Gratton, *Redefining personal information in the context of the Internet*, th. Paris II et Montréal, 2012.

but ultime de cette protection[914]. Ce but serait de protéger les individus contre le « risque de dommage » pouvant résulter de la collecte, de l'utilisation et de la divulgation de leurs données[915]. À partir de cette affirmation, Madame Gratton affirme que seules les données dont le traitement présente un « risque de dommage » pour les individus devrait être protégées. Ainsi, la qualification de donnée à caractère personnel devrait être restreinte aux seules données dont le traitement risque d'engendrer un dommage[916].

250. Critique. Une telle approche présente plusieurs avantages. D'abord, elle permet de circonscrire la notion de donnée à caractère personnel en proposant un critère excluant de son champ d'application certains types de données (les données les plus triviales et celles dont le traitement ne présente pas de « risque de dommage »[917]). Ensuite, elle est plus réaliste que l'approche *in abstracto* issue des règles actuelles puisqu'elle prend en compte la spécificité des traitements et leurs effets sur les personnes. Cette approche a également le bénéfice de s'intéresser aux capacités techniques réelles des responsables du traitement plutôt que de poser un standard abstrait applicable à tous les responsables du traitement[918].

Pour autant, l'approche fondée sur le dommage ne semble pas pouvoir prospérer, principalement pour deux raisons. D'une part, le postulat sur lequel repose cette théorie est contestable dès lors que le but des législations relatives aux données personnelles n'est pas uniquement de protéger les individus contre un « risque de dommage », mais vise aussi à s'assurer que les individus peuvent rester maîtres de leurs données et conscients, voire acteurs, des traitements effectués sur celles-ci[919]. Les droits des

---

[914] É. Gratton, *Redefining personal information in the context of the Internet*, th. Paris II et Montréal, 2012, p. 107 s.
[915] É. Gratton, *Redefining personal information in the context of the Internet*, th. Paris II et Montréal, 2012, p. 231.
[916] É. Gratton, *Redefining personal information in the context of the Internet*, th. Paris II et Montréal, 2012, p. 161.
[917] É. Gratton, *Redefining personal information in the context of the Internet*, th. Paris II et Montréal, 2012, p. 240.
[918] Le considérant 26 du règlement UE nº 2016/679 prévoit que pour « déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens *raisonnablement* susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement ». C'est bien un standard *in abstracto*, applicable à tous les acteurs, quelles que soient leur taille ou leurs capacités techniques, qui est utilisé pour déterminer si une donnée est personnelle, v. *supra,* nº 123.
[919] V. not. l'article premier de la loi nº 78-17 du 6 janv. 1978 et le considérant 7 du règlement UE nº 2016/679 qui reconnaissent aux personnes concernées un *pouvoir de contrôle* à l'égard de leurs données. V. aussi l'importance de la liberté d'autodétermination pour l'autonomie personnelle, v. *infra,* nº 397.

personnes concernées, notamment le droit d'être informé[920], le droit d'accès[921], le droit de rectification[922] ou encore le droit d'opposition[923] illustrent cet objectif législatif. Ainsi, l'approche fondée sur le dommage exclut de son domaine l'aspect lié au « développement individuel » que les protections de la vie privée et des données personnelles garantissent intrinsèquement[924]. Cet aspect est au cœur des dispositifs de protection élaborés par les jurisprudences de la Cour de cassation, de la CEDH, du Conseil constitutionnel et de la CJUE. D'autre part, cette approche présente une difficulté largement minimisée par son auteur : celle liée à la preuve du dommage[925]. Cette dernière peut s'avérer particulièrement difficile à rapporter pour les personnes concernées et être un obstacle à la mise en œuvre de cette théorie.

Centrer la notion de donnée personnelle autour du dommage revient, en réalité, à retenir une vision réparatrice de la protection des données personnelles et à ignorer un élément pourtant essentiel de cette protection : la volonté d'intervenir en amont de l'atteinte, justement pour en prévenir sa réalisation[926]. Pour résumer, cette théorie évite certaines des conséquences négatives d'une application généralisée de la notion. Toutefois, elle doit être exclue car elle risquerait d'écarter de la notion des données qui ne présenteraient pas un risque de dommage (ou pour lesquelles le risque de dommage ne pourrait pas être prouvé), mais qui auraient quand même des effets sur les personnes.

§ II. L'approche fondée sur le contrôle

251. Présentation. Dans sa thèse de 2011 sur les données personnelles, Madame Jessica Eynard distingue les informations nominatives des données à caractère personnel et propose de définir ces dernières comme « toute information saisissant par

---

[920] Initialement reconnue à l'article 27 de la loi nº 78-17 du 6 janv. 1978, puis par l'article 10 de la directive CE nº 95/46 et transposé dans l'article 32 de la loi française, l'obligation d'information figure désormais à l'article 13 du règlement UE nº 2016/679.
[921] Initialement reconnu à l'article 34 de la loi nº 78-17 du 6 janv. 1978, puis par l'article 12 de la directive CE nº 95/46 et transposé dans l'article 39 de la loi française, le droit d'accès est désormais prévu par l'article 15 du règlement UE nº 2016/679.
[922] Initialement reconnu à l'article 36 de la loi nº 78-17 du 6 janv. 1978, puis par l'article 12 de la directive CE nº 95/46 et transposé dans l'article 40 de la loi française, le droit de rectification figure désormais à l'article 16 du règlement UE nº 2016/679.
[923] Initialement reconnu à l'article 26 de la loi nº 78-17 du 6 janv. 1978, puis par l'article 14 de la directive CE nº 95/46 et transposé dans l'article 38 de la loi française, le droit d'opposition est désormais prévu par l'article 21 du règlement UE nº 2016/679.
[924] V. *infra*, nº 393.
[925] Sur le rôle préventif du droit des données à caractère personnel, v. not. P. Ancel, « La protection des données personnelles : aspects de droit privé français », *RID comp.* 1987, vol. 39, nº 3, p. 609, spéc. p. 618 ; v. *infra*, nº 551.
[926] V. *infra*, nº 321.

sa nature ou par son objet l'essence humaine biologique ou psychologique d'une personne physique identifiée ou identifiable et échappant intellectuellement et juridiquement à cette dernière »[927]. Deux critères cumulatifs émergent de cette définition : d'une part, la donnée doit *toucher à l'essence humaine*[928], et d'autre part, elle doit être *hors du contrôle de la personne*[929]. Selon son auteur, cette définition affranchirait la notion de donnée à caractère personnel des notions voisines et lui permettrait d'être véritablement autonome.

252. Critiques. Au-delà de l'intérêt conceptuel de cette définition et des apports de cette étude, les deux critères proposés semblent contestables. Le premier, fondé sur l'idée que la donnée doit toucher à l'essence humaine, encourage une conception large de celle-ci[930]. Si une donnée peut effectivement participer au reflet de l'identité ou de la personnalité, affirmer que toute donnée permet en elle-même de toucher à l'essence humaine s'avère une affirmation exagérée. Selon cette conception, une adresse IP pourrait aider à « cerner l'essence humaine » d'une personne puisqu'elle permettrait de la suivre et de construire, à travers son historique de navigation, une information particulièrement fine et détaillée sur elle[931]. Une telle affirmation est peu convaincante puisqu'ici, ce n'est pas l'adresse IP en tant que telle qui permet de cerner l'essence humaine, mais plutôt son traitement associé à d'autres données personnelles, et particulièrement son historique de navigation[932]. Interprétée aussi largement, la condition liée à « l'essence humaine » n'apporte pas les restrictions nécessaires au cantonnement de la notion. Selon l'auteur, le second critère, fondé sur l'absence de

---

[927] J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 184.
[928] J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 89 s.
[929] J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 141 s.
[930] J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 184.
[931] J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 19 s. et p. 98 s.
[932] L'accès à l'historique de navigation est loin d'être aussi aisé et répandu que l'accès à l'adresse IP d'une personne. En effet, seuls quelques acteurs avec lesquels la personne concernée entretient une relation contractuelle (par exemple, le navigateur ou le fournisseur d'accès à Internet) pourront effectivement avoir accès à cet historique. Par ailleurs, les sites accessibles *via* le protocole « https », c'est-à-dire avec une combinaison du protocole HTTP et une couche de chiffrement comme SSL ou TLS, garantissent une forme de confidentialité aux internautes puisque, dans cette situation, le fournisseur d'accès à Internet aura seulement connaissance du site visité mais ne connaîtra pas spécifiquement quelles pages ont été visitées sur ce site. Pour autant, il est certain que cet historique de navigation révèle de nombreuses informations sur la personne, v. L. Olejnik, C. Castelluccia et A. Janc, « Why Johnny can't browse in peace : on the uniqueness of web browsing history patterns », *5th Workshop on Hot Topics in Privacy Enhancing Technologies* 2012, Vigo. Plus récemment, v. S. Bird, I. Segall et M. Lopatka, « Replication : why we still can't browse in peace. On the uniqueness and reidentifiability of Web browsing histories », *6th Symposium on Usable Privacy and Security* 2020.

contrôle de l'intéressé, se révèlerait à deux égards : la perte de contrôle serait patente d'un point de vue intellectuel puisque soit la personne ignore complètement la donnée (car sa connaissance nécessite de maîtriser les codes informatiques)[933] ; soit parce que celle-ci ignore que ses faits et gestes ont été formalisés en informations[934]. Ce critère présente, lui aussi, certaines limites. Tout d'abord, il semble entrer en contradiction avec la philosophie générale du règlement européen, laquelle vise à éclairer les personnes sur les traitements de leurs données, notamment en renforçant les obligations d'information à la charge des responsables du traitement. Par ailleurs, un tel critère exclut de la notion tous les cas dans lesquels les personnes auxquelles se réfèrent les données ont une bonne maîtrise des codes informatiques et toutes les personnes ayant des connaissances détaillées des traitements effectués sur leurs données[935]. Cette proposition doctrinale pourrait donc avoir pour effet négatif d'encourager les personnes à rester passives face aux traitements de leurs informations et à ne pas percer les secrets de ces traitements puisque, s'ils le faisaient, leurs informations risqueraient de ne plus être couvertes par la notion.

Bien qu'utile à de nombreux égards, cette proposition ne répond pas aux problèmes identifiés. Une interprétation stricte de ces critères tend à exclure du champ d'application notionnel de nombreuses données ayant pourtant un lien avec des personnes physiques. À l'inverse, interprétés largement, les critères renforceraient encore davantage le mouvement d'expansion de la notion.

§ III. L'approche fondée sur le contexte

253. Présentation. Partant du constat que ce n'est pas tant le partage d'informations personnelles qui pose problème, mais plutôt le contexte dans lequel celui-ci est effectué[936], Madame Helen Nissenbaum a élaboré le concept original de *privacy in*

---

[933] J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 143 s.
[934] J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 148 s.
[935] Le manque de granularité de cette théorie en ce qui concerne la connaissance par la personne concernée est susceptible de poser quelques problèmes d'applicabilité. D'ailleurs, selon Madame Judith Rochfeld, plutôt que d'opposer connaissance ou ignorance du traitement, il faut plutôt « distinguer plusieurs degrés de conscience que la personne a de la collecte » de ses données, v. J. Rochfeld, « La vie tracée ou le code civil doit-il protéger la présence numérique des personnes ? », in *Mélanges J. Hauser*, LexisNexis et Dalloz, 2012, p. 619 s., n° 10, spéc. p. 629.
[936] H. Nissenbaum, *Privacy rights in context. Technology, policy, and the integrity of social life,* Stanford University Press, 2010, p. 142.

context[937]. Selon cette universitaire américaine, les attentes des individus à l'égard de leurs informations sont les mêmes, que le service soit numérique ou non[938] ; ce qui change fondamentalement avec le numérique, c'est l'échelle à laquelle les données sont collectées, analysées et partagées[939]. La protection de la *privacy* devrait donc s'adapter selon le contexte dans lequel les données sont traitées. Par exemple, s'il est parfaitement légitime pour un médecin d'avoir accès au dossier médical d'un patient, cet accès n'est pas justifié pour son assureur ou son employeur[940].

254. Critiques. Cette théorie présente plusieurs avantages, notamment celui d'ouvrir une discussion sur les attentes des personnes en ce qui concerne la protection de leurs données et le contexte dans lequel elles acceptent de partager leurs informations[941]. Ce débat s'inscrit parfaitement dans le droit américain de la protection de la *privacy*, lequel a régulièrement recours au concept de *reasonable expectations of privacy,* c'est-à-dire aux attentes raisonnables d'une personne en ce qui concerne la protection de sa vie privée[942]. D'ailleurs, Madame Helen Nissenbaum fonde sa théorie sur une critique du droit sectoriel américain protégeant certains types d'informations dans des secteurs d'activité[943].

Si cette approche est originale, elle fait reposer le système proposé sur un standard abstrait[944], lequel ne permet pas de prendre en compte les attentes subjectives des individus à l'égard de leurs informations personnelles[945]. Par ailleurs, elle se transpose difficilement dans le droit de l'Union européenne, notamment parce que les problèmes auxquels cette théorie se propose de répondre ne se posent pas dans les mêmes termes en Europe. Toutefois, le critère fondé sur le traitement peut servir de

---

[937] Madame Helen Nissenbaum est professeur de sciences de l'informatique à l'Université Cornell Tech aux États-Unis.
[938] H. Nissenbaum, « A contextual approach to privacy online », *Dædalus* 2011, vol. 140, p. 32 s., spec. p. 38.
[939] H. Nissenbaum, « A contextual approach to privacy online », *Dædalus* 2011, vol. 140, p. 32 s., spec. p. 37 s.
[940] H. Nissenbaum, *Privacy rights in context. Technology, policy, and the integrity of social life,* Stanford University Press, 2010, p. 146.
[941] H. Nissenbaum, *Privacy rights in context. Technology, policy, and the integrity of social life,* Stanford University Press, 2010, p. 129 s.
[942] La jurisprudence qui s'est développée sur le fondement du Quatrième amendement en est la preuve, v. not. S. Jones, « Reasonable expectations of privacy : searches, seizures, and the concept of Fourth amendment standing », *University of Memphis Law* Review 1997, vol. 27, p. 907 s. [27 U. MEM. L. REV. 907].
[943] H. Nissenbaum, « A contextual approach to privacy online », *Dædalus* 2011, vol. 140, p. 32 s., spec. p. 39.
[944] D. Gutmann, *Le sentiment d'identité. Étude de droit des personnes et de la famille*, th. Paris II, 2000, LGDJ, n° 263, p. 230.
[945] Certaines personnes peuvent avoir une vision différente (c'est-à-dire plus ou moins restrictive) de la protection qu'ils attendent de leurs données. Pour Madame Helen Nissenbaum, ce problème peut être réglé grâce au régime du consentement éclairé, v. H. Nissenbaum, « A contextual approach to privacy online », *Dædalus* 2011, vol. 140, p. 32 s., spec. p. 45.

source d'inspiration pour une nouvelle approche européenne de la notion de donnée à caractère personnel.

SECTION II – LE CARACTÈRE OPPORTUN DE L'APPROCHE TÉLÉOLOGIQUE

255. Plan. Bien que ces propositions doctrinales illustrent la complexité du droit des données à caractère personnel, elles ne répondent pas aux besoins d'encadrement du domaine de la notion de donnée à caractère personnel. L'expansion de la notion ne peut pas continuer de perdurer : un nouveau critère entourant la donnée à caractère personnel doit donc être proposé. L'exposé de la proposition (Sous-section I) précèdera l'analyse de ses bénéfices (Sous-section II).

SOUS-SECTION I – EXPOSÉ DE LA PROPOSITION

256. Une nouvelle définition fondée sur les distinctions classiques. La notion actuelle a l'avantage d'avoir su s'adapter aux évolutions technologiques, et une refonte complète risquerait de fragiliser la mise en œuvre de ce droit. Ainsi, plutôt que de continuer d'élargir la notion de donnée à caractère personnel et pour éviter qu'elle ne devienne le réceptacle de toutes les données, il convient de proposer un critère pour l'encadrer. La nouvelle définition reprend les balancements classiques entre les informations directement identifiantes – ou relatives à une personne identifiée – et les informations indirectement identifiantes. Comme en droit positif, lorsque les données sont intrinsèquement liées à une personne (par leur nature ou par leur mode de collecte), elles entrent naturellement dans la notion de donnée à caractère personnel. En revanche, lorsque la donnée est indirectement identifiante, elle doit recevoir la qualification de donnée à caractère personnel seulement lorsque son traitement établit un lien entre la donnée et la personne. Le traitement est donc érigé comme le critère central de l'opération de qualification des données indirectement identifiantes.

257. Objectifs de la proposition. Cette proposition tente de concilier deux objectifs : celui de protéger les données pour lesquelles un rapprochement entre la donnée et la personne existe (soit par *nature* soit du fait d'un *traitement*), et celui de permettre la circulation des informations indirectement liées à des personnes physiques. En dehors de ces deux catégories, et conformément à la définition actuelle de donnée à caractère

personnel, les données qui ne concernent pas ou ne concernent plus une personne physique sont exclues de la notion. Il en va ainsi des simples données et des données anonymisées[946].

258. Plan. Les données directement identifiantes font *par nature* référence à une personne physique. Dès lors, elles sont incontestablement liées à une personne physique et doivent donc entrer dans le domaine de la donnée à caractère personnel. Pour ces données, l'approche téléologique n'est pas nécessaire (§ I). En revanche, lorsque les données sont indirectement identifiantes, c'est-à-dire que l'identification est le fruit d'un traitement particulier, cette approche se révèle particulièrement utile (§ II).

§ I. L'absence de nécessité de l'approche téléologique pour les données identifiantes

259. Une protection automatique des données directement identifiantes. Sur le modèle du droit positif, il est évident que toutes les données directement identifiantes, c'est-à-dire celles dont la *fonction* est d'identifier une personne physique[947], sont couvertes par la notion de donnée à caractère personnel. Nous l'avons vu, les données directement identifiantes sont principalement celles relatives à l'état des personnes[948]. Celui-ci se compose spécialement des données de l'état-civil et visent l'identité civile de la personne[949]. Relèvent ainsi de l'état des personnes le nom, les prénoms, la date, l'heure et le lieu de naissance, le sexe, la couleur des yeux, le domicile ou la résidence, l'image numérisée du visage, les empreintes digitales[950]… Puisque ces données entretiennent un lien intrinsèque avec la personne, elles permettent de la reconnaître et de la différencier des autres : elles ont donc pour effet de l'identifier[951]. Dès lors, elles entrent évidemment dans la notion de donnée à caractère personnel. À cet égard, la

---

[946] Nous préférons distinguer les simples données (c'est-à-dire celles qui n'ont pas de lien avec une personne) des données anonymisées (qui sont les données sur lesquelles un traitement a été effectué en vue de retirer suffisamment d'éléments pour que la personne concernée ne puisse plus être identifiée), v. *supra*, n° 124.
[947] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, n° 492, p. 216.
[948] V. *supra,* n° 112.
[949] F. Terré et D. Fenouillet, *Droit civil. Les personnes*, 8e éd., Dalloz, 2012, n° 126, p. 140.
[950] Ces données font partie de celles nécessaires à l'établissement des cartes nationales d'identité, v. décret n° 2016-1460 du 28 oct. 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité, *JORF* 30 oct. 2016, n° 0254, texte n° 18.
[951] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *V°* « Identité », sens 1.

définition proposée n'apporte pas de changement à l'approche actuelle concernant ces données. Pour autant, et comme le montre d'ores et déjà la jurisprudence dans cette matière, le contexte occupe une place importante.

260. Une précaution : la place du contexte. Bien entendu, il ne s'agit pas de soumettre à la notion de donnée à caractère personnel toutes les données dont la fonction est de permettre, de manière abstraite, l'identification. L'objectif est plutôt de s'assurer que « l'ensemble des caractéristiques biologiques et sociales permettant d'individualiser » les personnes au sein d'un groupe relèvent bien de la notion[952]. Ainsi, même si certaines données sont par nature directement identifiantes, en pratique, le contexte occupe un rôle essentiel pour permettre d'identifier une personne[953]. Par exemple, si un nom est considéré comme une donnée directement identifiante, encore faut-il que celui-ci puisse, dans le contexte dans lequel il est traité, être rattaché à une personne. C'est d'ailleurs l'interprétation retenue dans une décision du tribunal de grande instance de Paris[954]. Dans cette affaire, relative à un fichier de généalogie composé exclusivement de patronymes par ville, le juge des référés avait considéré que la simple présence d'un nom dans un fichier ne suffisait pas à entraîner l'application de la loi Informatique et libertés. C'est également l'interprétation retenue pour la diffusion des fichiers de prénoms qui sont établis à partir des bulletins de naissance de personnes nées en France. Ces fichiers sont souvent utilisés pour établir des courbes de popularité des prénoms ainsi que des cartes départementales des prénoms choisis, ou encore le taux de réussite de certains prénoms au baccalauréat[955]. Pourtant, selon une interprétation stricte de la notion de donnée directement identifiante, le prénom relèverait bien de son domaine puisqu'il est un élément d'identification au sein d'un groupe[956]. Une interprétation plus raisonnable considère que les données contenues dans ces fichiers ne sont pas des données directement identifiantes. En effet, le prénom tel qu'utilisé dans ce fichier ne permet pas d'identifier, au sein d'un groupe, une

[952] F. Zenati-Castaing et T. Revet, *Manuel de droit des personnes*, PUF, 2006, n° 33, p. 49.
[953] Le contexte est ici entendu comme le contexte du traitement et ne fait pas référence à la théorie développée par Madame Helen Nissenbaum et exposée précédemment, v. H. Nissenbaum, « A contextual approach to privacy online », *Dædalus* 2011, vol. 140, p. 32 s., spec. p. 38.
[954] TGI Paris, réf., 22 sept. 2008, *Kalid O.* c. *NotreFamille.com*.
[955] Monsieur Baptiste Coulmont est un sociologue spécialisé dans la sociologie des prénoms. Ses travaux utilisent souvent les bases de données des prénoms mises à disposition par les autorités et ont montré les taux de réussite des prénoms au baccalauréat ou les prénoms les plus attribués selon les départements, v. not. B. Coulmont, « Le prénom : catégorie sociale. Baccalauréat ».
[956] B. Teyssié, *Droit des personnes*, 21e éd., LexisNexis, 2019, n° 467, p. 342.

personne. Au mieux, il renseigne sur la popularité du prénom, ou enrichit les études sur la sociologie des prénoms[957]. Des précautions sont prises afin d'éviter de pouvoir inférer des informations particulières sur certaines personnes lors de l'établissement de ces fichiers. Les prénoms rarement attribués n'y sont donc pas intégrés[958].

Ainsi, et conformément au droit positif, le contexte occupe une place importante dans la qualification d'une donnée directement identifiante[959].

261. Une protection automatique des données à caractère personnel pour les données d'une personne identifiée. À l'instar de ce que prévoit le droit positif, notre proposition considère que les données relatives à une personne identifiée relèvent également de la notion de données à caractère personnel. Selon l'interprétation que nous avons proposée précédemment, cette catégorie de données fait référence aux informations concernant une personne qui s'est identifiée, notamment *via* un formulaire ou un profil utilisateur[960]. Dans l'environnement numérique, il s'agit des données générées par l'activité de la personne identifiée. Ainsi, lorsqu'une entreprise suit les activités de ses utilisateurs connectés (sur et en dehors de son site), comme c'est le cas de Facebook[961] ou Google[962], les données générées par ces activités entrent dans la notion de donnée à caractère personnel.

Pour résumer, la proposition de définition reprend les principes du droit positif applicables aux données directement identifiantes. Ainsi, les données directement identifiantes et celles relatives à une personne identifiée entrent dans la notion de données à caractère personnel.

---

[957] B. Coulmont, *Sociologie des prénoms*, La Découverte, 2014.
[958] Les prénoms très rares, c'est-à-dire les prénoms attribués moins de trois fois sur une année ou ceux attribués moins de vingt fois entre les périodes allant de 1900 à 1945 et entre 1946 à 2017, sont retirés de ces fichiers, INSEE, « Fichier des prénoms », Documentation, 2019.
[959] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 502, p. 222.
[960] V. *supra,* nº 113.
[961] Facebook utilise les données provenant de sites tiers ou d'applications intégrant des modules tels que les boutons « J'aime », « Se connecter » ou ses pixels (qui sont des éléments de code logiciel). V. not. J. Lausson, « Facebook sait tout ce que vous faites sur le web : comment désactiver le ciblage des sites », *Numerama* 30 janv. 2020.
[962] Pour s'en convaincre il suffit de se connecter à un compte Google et d'aller dans l'onglet « Mon activité » dans lequel figure des données nombreuses et variées collectées par l'entreprise.

§ II. L'utilité de l'approche téléologique pour les données indirectement identifiantes

262. Une identification possible. Pour qu'une donnée indirectement identifiante soit considérée comme se rapportant à une personne, il est nécessaire d'en faire un traitement particulier *ou* d'ajouter certaines informations supplémentaires[963]. En effet, ces données n'ont pas, en elle-même, une fonction d'identification comme c'est le cas pour les données directement identifiantes. Ainsi, le lien avec la personne est possible, mais uniquement sous certaines conditions. Personne n'oserait affirmer que, de manière abstraite, un numéro d'abonné, une puce ou un numéro d'identifiant telle qu'une adresse MAC sont des données qui, en tant que telles, se rapportent à une personne. C'est bien lorsque ces données font l'objet d'un traitement qu'elles peuvent, dans certains cas, renseigner sur la personne. Le traitement devrait donc occuper une place plus importante dans l'opération de qualification de ces données. Pourtant, les règles actuelles ne s'intéressent au traitement qu'après avoir préalablement vérifié la présence de données à caractère personnel. Il est tout de même possible de détecter un timide mouvement valorisant la place du traitement dans le droit des données personnelles. Ce mouvement ne devrait-il pas être renforcé, voire pleinement consacré ?

263. Plan. Les manifestations de la prise en compte du traitement montrent que le critère proposé est déjà en germe dans le droit positif (A). Il convient de consacrer pleinement le traitement comme un critère de qualification pour les données indirectement identifiantes (B).

A. Manifestations de la place croissante du traitement dans le droit positif

264. Plan. Selon une opinion doctrinale, « le Régulateur vise aujourd'hui les "données à caractère personnel" non plus tant par rapport à la personne sur laquelle elles portent mais par rapport à l'usage qui en est fait, ou pour lequel la "donnée" a été prélevée, traitée et conservée »[964]. Cette affirmation témoigne du besoin que ressent la

[963] Le terme « ou » doit être ici entendu au sens mathématique, c'est-à-dire au sens non exclusif (disjonction logique) : au moins une des deux assertions est vraie.
[964] M.-A. Frison-Roche, « Penser le monde à partir de la notion de "donnée" », in *Internet, espace d'interrégulation*, dir. M.-A. Frison-Roche, Dalloz, 2016, p. 8.

doctrine, pour comprendre l'évolution de la donnée à caractère personnel, de s'intéresser à la réalité des traitements et non plus seulement à la notion abstraite de donnée à caractère personnel. Cette analyse révèle plusieurs signes qui témoignent d'une meilleure prise en considération du traitement. Dans certains cas, la finalité du traitement permet la diffusion de données indirectement identifiantes (1), dans d'autres situations, elle sert à caractériser l'atteinte à la vie privée (2). Plus rarement, l'analyse de la finalité du traitement a été utilisée pour exclure des données indirectement identifiantes de la notion de donnée à caractère personnel (3).

1. La finalité du traitement pour permettre la diffusion de données ouvertes indirectement identifiantes

265. Les données de jurisprudence. Dans une démarche d'ouverture et de libre réutilisation des données générées par l'activité des services publics, les administrations participent au mouvement d'*open data* en mettant à disposition leurs bases de données. De manière exceptionnelle, certaines bases de données peuvent contenir des données indirectement identifiantes. C'est notamment le cas des bases de données des décisions de justice.

Malgré leur lien indirect avec des personnes physiques, ces décisions de justice présentent un intérêt majeur pour le public[965]. Elles sont le corollaire, à l'ère numérique, du principe de publicité de la justice qui s'inscrit de longue date dans la tradition juridique française[966]. En effet, la libre circulation de ces données participe au renforcement de la confiance des citoyens dans leur justice et ouvre d'importantes perspectives pour l'étude de l'activité des juridictions[967]. Historiquement, l'accès à l'information juridique était relativement limité, même si l'apparition des Bulletins

---

[965] Les expressions « données d'intérêt général » ou « données de référence » peuvent être utilement invoquer pour ces bases de données de décisions de justice. En effet, elles reflètent l'aspect démocratique propre à ces données. Selon Madame Lucie Cluzel-Métayer, les données d'intérêt général « renvoient essentiellement à un critère organique » et elles ne sont pas synonymes des données de référence qui visent « les données qui sont susceptibles de faire l'objet d'une utilisation fréquente par un nombre d'acteurs tant publics que privés et dont la qualité, en termes notamment de précision, de fréquence de mise à jour ou d'accessibilité, est essentielle pour ces utilisations », L. Cluzel-Métayer, « Les limites de l'open data », *AJDA* 2016, p. 102. Ces deux types de données ont été consacrées par la loi nº 2016-1321 du 7 oct. 2016 pour une République numérique (respectivement aux articles 17 s. et 14).

[966] L. Cadiet, « L'open data des décisions de justice. Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice. Rapport à la garde des Sceaux », 2017, p. 23. Dans ce rapport, Monsieur Loïc Cadiet fait référence à la loi des 16 et 24 août 1790 laquelle prévoyait, dans son article 14, que « en toute matière civile ou criminelle, les plaidoyers, rapports et jugements seront publics ». Ce principe de publicité a été constitutionnalisé dans l'article 208 de la Constitution du 5 fructidor An III qui disposait que « les séances des tribunaux sont publiques [...] les jugements sont prononcés à haute voix ».

[967] L. Cadiet, « L'open data des décisions de justice. Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice. Rapport à la garde des Sceaux », 2017, p. 19.

officiels a contribué à sa meilleure diffusion[968]. Le lancement du site Légifrance en 1999, conçu comme un véritable service public, ouvre au grand public l'accès aux données juridiques[969]. En reconnaissant à chacun la possibilité de consulter les lois, les textes règlementaires ou les décisions de justice, ce site a incontestablement permis une meilleure information du public et a renforcé l'accès au droit[970]. Pour autant, comme certaines décisions de justice contiennent des données personnelles, la CNIL a recommandé que leur mise à disposition sur le site Légifrance se fasse après le retrait des nom et adresse des parties ou témoins[971].

En 2014, lorsqu'il a été question d'ouvrir, en *open data,* les bases de données des décisions de justice alimentant le site Légifrance, la question de la protection des données indirectement identifiantes s'est posée[972]. En effet, la consultation par requête individuelle du site Légifrance rendait les recoupements de données plus difficiles que ceux permis par le téléchargement complet de ces bases de données. L'ouverture en *open data* de ces bases de données facilitait la mise en œuvre de traitements de données à des fins de réidentification des personnes. Pour garantir un équilibre entre la mise à disposition de ces bases de données et les principes de protection des données personnelles, un *caveat*, c'est-à-dire une mise en garde, a accompagné leur licence de réutilisation[973]. Ce *caveat* précisait que lorsqu'une information publique contient des données personnelles qui « ont, préalablement à leur diffusion, fait l'objet d'une anonymisation totale ou partielle, (…) la réutilisation ne peut avoir pour *objet ou pour effet* de réidentifier les personnes concernées »[974]. Ainsi, le critère retenu pour permettre la diffusion de ces données et encadrer leur réutilisation était un critère téléologique : tous les traitements sur ces données sont possibles sauf ceux qui auraient *pour objet ou pour effet* de réidentifier les personnes physiques. Même si la publication

---

[968] L. Cadiet, « L'open data des décisions de justice. Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice. Rapport à la garde des Sceaux », 2017, p. 23.
[969] Arrêté du 6 juill. 1999 relatif à la création du site Internet Légifrance, *JORF* 13 juill. 1999, nº 160, p. 10406.
[970] S. Lasvignes, « Discours. Conférence de Paris sur l'open data et le gouvernement », 24 avr. 2014.
[971] CNIL, délibération nº 01-057 du 29 novembre 2001 portant recommandation sur la diffusion de données personnelles sur Internet par les banques de données de jurisprudence, et le bilan de son application, CNIL, Bilan de l'application de la recommandation de la Commission nationale de l'informatique et des libertés du 29 novembre 2001 sur la diffusion de données personnelles sur Internet par les banques de données de jurisprudence : pour un encadrement législatif renforçant la protection des données à caractère personnel en matière de diffusion de décisions de justice,19 janv. 2006.
[972] En effet, certaines décisions de justice contiennent des données indirectement identifiantes dans la mesure où y figurent des noms et adresses de personnes physiques qui ont été occultés. Une anonymisation complète de ces décisions de justice les rendrait incompréhensibles et inutilisables puisqu'il faudrait retirer tous les éléments de fait permettant à une personne qui connaîtrait l'une des parties de pouvoir la réidentifier.
[973] CNIL, « Ouverture des jeux de données de jurisprudence de Légifrance », 16 sept. 2015.
[974] Premier ministre, « Avertissement – Données à caractère personnel » accompagnant les bases de données de jurisprudence.

complète de ces bases de données continue à faire débat[975], le critère téléologique retenu en 2015 pour leur mise à disposition montre une meilleure prise en considération de la finalité des traitements. D'ailleurs, l'utilité du critère de finalité du traitement s'est confirmée à plusieurs reprises, notamment à l'occasion de la publication des données foncières.

266. Les données foncières. En avril 2019, le ministère de l'Action et des Comptes Publics a publié une base de données relatives aux valeurs foncières, recensant l'ensemble des ventes de biens fonciers réalisées au cours des cinq dernières années. Cette publication visait à améliorer la transparence des marchés financiers et immobiliers[976] et la connaissance des prix sur le marché immobilier[977]. Parmi ces données figurent notamment l'adresse du bien, son descriptif, et son prix de vente. Certaines de ces données se rapportent donc, indirectement, à des personnes physiques puisqu'elles permettent de déterminer le prix d'achat d'un bien par une personne ou la surface exacte de son bien, particulièrement lorsque ces données sont croisées avec celles du cadastre. Sur le modèle du *caveat* associé à la publication des bases de données des décisions de justice, l'article R. 112 A-3 du livre des procédures fiscales prévoit que les traitements de ces données « ne peuvent avoir ni pour objet ni pour effet de permettre la réidentification des personnes concernées ». Ici encore, c'est un critère relatif à la finalité du traitement ou aux effets de celui-ci qui a été retenu pour permettre une circulation des données indirectement identifiantes. Dans ces deux situations, ce critère a été choisi pour valoriser la circulation de données indirectement identifiantes, tout en interdisant une réidentification des personnes. Une telle circulation est d'autant plus justifiée que ces données présentent un risque faible d'atteinte à la personne. Ainsi, l'analyse de la finalité du traitement permet, dans la mise en œuvre de la politique de

---

[975] Le débat sur les modalités de diffusion de ces décisions continue d'être houleux. Si la loi pour une République numérique de 2016 avait consacré un principe de diffusion en *open data* de ces décisions, ce texte n'a jamais été mis en œuvre. Le ministère de la Justice avait chargé Monsieur Loïc Cadiet de rédiger un rapport sur le sujet, v. L. Cadiet, « L'open data des décisions de justice. Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice. Rapport à la garde des Sceaux », 2017. En mars 2019, le législateur a modifié en profondeur le régime de publicité, v. not. J. Jourdan-Marques, « La publicité des décisions, une garantie émoussée ? », séminaire *L'avenir du procès civil* du Centre de recherche sur la Justice et le règlement des conflits de l'Université Paris II Panthéon Assas, *JCP G* 2019, supplément au nº 14, p. 62 ; N. Blanc et P.-Y. Gautier, « Contre "l'anonymisation" des arrêts publiés : décadence des références de jurisprudence », *D.* 2019, p. 1648. Le nouveau régime distingue entre l'*open data* des décisions et l'accès aux décisions, v. not. B. Cassar, « La distinction entre l'open data et l'accès aux décisions de justice », *Dalloz actualité* 19 juill. 2019. Sur la diffusion des décisions de justice rendues en matière familiale, v. E. Buat-Ménard, « Open data des décisions de justice rendues en matière familiale », *AJ Fam.* 2019, p. 330.

[976] Art. L. 112 A du livre des procédures fiscales.

[977] Ministère de l'Action et des Comptes Publics, « Communiqué de presse : Gérald Darmanin annonce la publication et l'ouverture en open data des données foncières à l'occasion d'un hackathon à Bercy », 24 avr. 2019.

mise à disposition des données ouvertes, de contourner les obligations de confidentialité applicables aux données indirectement identifiantes et de laisser les tiers accéder à ces données.

2. La finalité du traitement pour caractériser l'atteinte à la vie privée

267. Exemples de jurisprudences du Conseil constitutionnel. Le Conseil constitutionnel s'est intéressé à la finalité du traitement pour protéger, sur le fondement du droit au respect de la vie privée, des données indirectement identifiantes. Si, dans un premier temps, le Conseil constitutionnel a refusé de considérer que la communication de données de connexion pouvait caractériser une atteinte à la vie privée[978], il a progressivement fait évoluer cette interprétation en s'intéressant aux traitements effectués sur ces données. Le Conseil constitutionnel a finalement retenu que la communication des données de connexion, c'est-à-dire celles portant sur « l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux »[979], était de nature à porter atteinte au droit au respect de la vie privée de la personne intéressée. Ainsi, c'est bien parce que les données sont traitées dans le but d'identifier une personne que le Conseil constitutionnel a considéré qu'elles relevaient du domaine de la vie privée. Ce raisonnement a été confirmé dans une décision du 22 mars 2012 par laquelle le Conseil constitutionnel était invité à se prononcer sur l'intégration des données biométriques dans la notion de vie privée. Pour retenir l'atteinte à la vie privée, le Conseil ne s'est pas seulement intéressé aux données en elles-mêmes, mais a surtout analysé les caractéristiques du traitement[980]. Le Conseil constitutionnel avait alors retenu que

---

[978] À l'égard des services fiscaux, des services douaniers et de l'AMF, v. Cons. const., 27 déc. 2011, n° 2001-457 DC, cons. 8 ; à l'égard de la HADOPI, v. Cons. const., 10 juin 2009, n° 2009-580 DC, cons. 27 s. ; à l'égard des services des douanes, v. Cons. const., 27 janv. 2012, n° 2011-214 QPC, cons. 3. Sur cette évolution v. N. Martial-Braz, « Inconstitutionnalité du droit de communication des données de connexion reconnu à l'AMF », *Revue des Sociétés* 2017, p. 582. Une question préjudicielle vient d'être posée à la CJUE dans le cadre de ce contentieux pour savoir si le droit de l'Union européenne autorise de différer les effets de l'incompatibilité constatée avec le droit autorisant l'AMF à obtenir sans autorisation d'une autorité indépendante la communication des données de connexion, v. Cass. crim., 1er avril 2020, n° 19-80.900, *NBP,* pour une analyse de ces questions, v. E. Dezeuze et C. Méléard, « Enquêtes et poursuites en matière d'abus de marché », *Revue des Sociétés* 2020, p. 556.

[979] Cons. const., 21 juill. 2017, n° 2017-647 QPC, cons. 9.

[980] N. Ochoa, *Le droit des données personnelles, une police administrative spéciale*, th. Paris I, 2014, p. 415.

compte tenu de l'objet du traitement[981], ainsi que de la nature des données et des caractéristiques techniques du fichier, l'atteinte à la vie privée était constituée[982].

Lorsqu'il a été appelé à se prononcer sur la constitutionnalité de la consultation des listes de soutiens aux référendums, le Conseil constitutionnel a également retenu une analyse téléologique pour étudier l'atteinte à la vie privée[983]. La création de ces listes implique la mise en œuvre d'un traitement de données à caractère personnel mentionnant les opinions politiques des personnes concernées[984]. Pour déterminer si l'enregistrement des soutiens et sa consultation s'opéraient dans le respect du droit au respect de la vie privée, le Conseil constitutionnel a relevé que le législateur « a interdit que les données à caractère personnel collectées à l'occasion du recueil des soutiens puissent être utilisées à d'autres fins que celles définies par la loi organique »[985]. Le juge constitutionnel s'intéresse donc régulièrement aux finalités des traitements pour se prononcer sur l'atteinte à la vie privée. La Cour de justice prend aussi en compte ce critère.

268. Exemples de jurisprudences de la Cour de justice de l'Union européenne. La CJUE a également adopté, à plusieurs reprises, une approche téléologique pour caractériser l'atteinte à la vie privée. Au sujet de la qualification des métadonnées, la CJUE a, elle aussi, considéré que la conservation des « données nécessaires pour retrouver et identifier la source d'une communication et la destination de celle-ci, pour déterminer la date, l'heure, la durée et le type d'une communication, le matériel de communication des utilisateurs, ainsi que pour localiser le matériel de communication mobile, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP pour les services Internet » aux fins de leur accès éventuel par les autorités nationales compétentes, concerne « de manière directe et spécifique la vie privée »[986]. En l'espèce, la Cour a effectué une analyse *in concreto*

---

[981] Cons. const., 22 mars 2012, nº 2012-652 DC, cons. 10.
[982] Cons. const., 22 mars 2012, nº 2012-652 DC, cons. 11.
[983] L'article 11, alinéa 3 de la Constitution prévoit que le référendum peut être organisé « à l'initiative d'un cinquième des membres du Parlement, soutenue par un dixième des électeurs inscrits sur les listes électorales. Cette initiative prend la forme d'une proposition de loi et ne peut avoir pour objet l'abrogation d'une disposition législative promulguée depuis moins d'un an ». V. Cons. const., du 5 déc. 2013, nº 2013-681 DC, cons. 28.
[984] Commentaire de la décision du Conseil constitutionnel, 5 déc. 2013, nº 2013-681 DC, p. 15.
[985] Cons. const., 5 déc. 2013, nº 2013-681 DC, cons. 28.
[986] CJUE, 8 avril 2014, *Digital Rights Ireland Ltd* c. *Minister for communications et al. et Kärntner Landersregierung*, C-293/12 et C-594/12, § 26 s. ; CJUE, 6 oct. 2020, *La Quadrature du Net* c. *Premier ministre*, C-511/18, C-512/18 et C-520/18, § 117. V. aussi CEDH, 3 avril 2007, *Copland* c. *Royaume-Uni*, nº 62617/00, § 43 s. qui s'intéresse également aux finalités de la conservation des données.

des traitements et s'est attardée sur leurs finalités. Elle a également remarqué les risques de cette collecte, laquelle permet d'obtenir des informations très précises concernant la vie privée des personnes telles que leurs habitudes de vie quotidienne, leurs lieux de séjour permanents ou temporaires, leurs déplacements journaliers, leurs activités, leurs relations sociales et les milieux sociaux qu'elles fréquentent[987]. Ainsi, c'est l'analyse de la finalité du traitement qui a encouragé la CJUE à retenir l'atteinte à la vie privée.

3. La finalité du traitement pour qualifier des données indirectement identifiantes

269. Exemples de jurisprudences du Conseil d'État. La jurisprudence du Conseil d'État a exclu, à plusieurs reprises, certaines données indirectement identifiantes de la notion de donnée à caractère personnel. Cette exclusion s'est fondée sur l'analyse du traitement effectué sur les données, lequel n'établissait pas de lien avec une personne physique. En effet, le Conseil d'État a été saisi de la qualification de données de connexion, et il a refusé de leur reconnaître le statut de données à caractère personnel. Pour fonder cette exclusion, la Haute juridiction administrative avait affirmé que l'enregistrement de données de connexion à des fins statistiques ne constituait pas un traitement de données à caractère personnel[988]. La juridiction suivait les conclusions de son rapporteur public qui avait considéré que « l'administration n'a mis en œuvre aucun traitement *spécifique* de données de connexion sur les pages d'information vers lesquelles sont redirigés les utilisateurs » et que « ces pages d'information ne font pas l'objet d'un traitement *particulier* – et notamment pas d'un traitement visant à réidentifier les utilisateurs »[989]. Ainsi, le Conseil d'État a retenu une approche *téléologique* pour exclure de la notion de donnée à caractère personnel des données indirectement identifiantes lorsque leur traitement n'avait pas pour finalité d'établir un lien avec la personne.

Plutôt que de continuer à accepter des entorses à la qualification légale de donnée à caractère personnel, il convient de consacrer le traitement comme un critère de qualification pour les données indirectement identifiantes.

---

[987] CJUE, 8 avril 2014, *Digital Rights Ireland Ltd* c. *Minister for communications et al. et Kärntner Landersregierung*, C-293/12 et C-594/12, § 27 ; CJUE, 6 oct. 2020, *La Quadrature du Net* c. *Premier ministre*, C-511/18, C-512/18 et C-520/18, § 117.
[988] CE Sec.,18 juin 2018, *Société La Quadrature du Net et autres*, nº 406083, inédit *Lebon*.
[989] G. Odinet, concl. ss CE Sec., 18 juin 2018, *Société La Quadrature du Net et autres*, nº 406083.

B. Consécration du traitement comme critère de qualification pour les données indirectement identifiantes

270. Plan. L'exposé du traitement comme critère d'application (1) précédera celui de sa délimitation (2).

1. Exposé du critère

271. La finalité du traitement. Monsieur Daniel Gutmann le formulait parfaitement : « identifier un individu, c'est déjà porter atteinte à sa vie privée »[990]. Le fait d'opérer un rapprochement entre une information et une personne caractérise donc l'atteinte que le droit des données à caractère personnel entend réglementer. Pour les données indirectement identifiantes, cette identification passe immanquablement par un traitement spécifique de la donnée. Conformément à cette logique, il convient de retenir, pour les données indirectement identifiantes, une approche téléologique.

272. L'approche téléologique. Le Vocabulaire juridique de l'Association Henri Capitant définit l'adjectif téléologique comme celui qui « se rapporte à la science des fins, à la connaissance des finalités »[991]. Parler d'approche téléologique en matière de donnée à caractère personnel revient donc à faire dépendre la qualification de la donnée de la finalité du traitement effectué sur celle-ci.

273. Formulation de la proposition. Selon l'approche proposée, lorsque *le traitement effectué sur la donnée a pour objet ou pour effet d'établir un lien avec une personne physique*, la donnée indirectement identifiante doit recevoir la qualification de donnée à caractère personnel[992]. À l'inverse, lorsque le traitement effectué sur la donnée ne vise pas ou n'a pas pour effet d'établir un tel lien, la prudence et l'efficacité juridique commandent que celle-ci ne soit pas considérée comme une donnée à caractère personnel, et ce même si un autre responsable pourrait mettre en œuvre un tel

---

[990] D. Gutmann, *Le sentiment d'identité. Étude de droit des personnes et de la famille*, th. Paris II, 2000, LGDJ, n° 381, p. 317. Certes, dans cette affirmation, le terme « identifier » était plutôt utilisé pour faire référence à l'identité, c'est-à-dire au fait de nommer une personne, de lui donner un nom et un prénom. Toutefois, le phénomène d'identification ne se limite plus au lien qu'une personne entretient avec son nom ; c'est d'ailleurs l'une des raisons qui ont poussé le législateur à abandonner la notion d'information nominative. Sur le glissement sémantique de l'information nominative à la donnée à caractère personnel, v. *supra,* n° 138.
[991] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *V°* « Téléologique ».
[992] C'est aussi la conclusion à laquelle arrive Madame Christina Koumpli au sujet de la qualification de données sensibles, v. C. Koumpli, *Les données personnelles sensibles. Contribution à l'évolution du droit fondamental à la protection des données à caractère personnel*, th. Paris I, 2019, p. 228 s.

traitement. Évidemment, si ce tiers fait sur cette donnée indirectement identifiante un traitement qui a pour objet ou pour effet de faire un lien entre l'information et une personne physique, il doit être considéré comme effectuant un traitement des données à caractère personnel[993]. Pour mieux comprendre comment doit être interprété le critère proposé, il convient d'en préciser les termes.

2. Délimitation du critère

274. Rappel du critère. Le critère proposé prévoit qu'une donnée indirectement identifiante dont *le traitement a pour objet ou pour effet d'établir un lien avec une personne physique* doit être qualifiée de donnée à caractère personnel.

275. Précisions concernant la référence au traitement ayant « pour objet ». Selon le dictionnaire de l'Académie française, le terme objet a une double signification. Dans sa première acception, l'objet est « ce qui s'offre à la perception » ; dans sa seconde, l'objet est « ce sur quoi porte une faculté, un sentiment »[994]. C'est plutôt dans cette seconde acception que la notion d'objet, au sens de la définition proposée, doit être entendue. Une telle conception rapproche ce terme de l'idée d'objectif qui s'entend comme « le but que l'on cherche à atteindre »[995], ou du terme finalité qui se rapporte au « caractère de ce qui est subordonné à une fin, tend à un but »[996]. En droit, le terme objet renvoie, le plus souvent, à une idée similaire. En droit des contrats par exemple, l'objet du contrat désigne l'opération juridique que les parties ont voulu effectuer[997]. Quant à l'objectif, en matière contractuelle, ce terme renvoie au résultat qu'une partie fait obligation à l'autre d'atteindre[998], et en politique législative il s'agit de la fin pour laquelle est ordonnée une réforme[999].

---

[993] Cette conception fait écho aux débats rappelés par l'arrêt *Breyer* dans lequel la CJUE a discuté du critère à prendre en compte pour déterminer si une personne est identifiable. La Cour s'interrogeait pour savoir si le critère utilisé devait être un critère « objectif » ou « relatif ». En application du critère « objectif », il suffit qu'une seule personne (un tiers ou le responsable du traitement) soit en mesure de déterminer l'identité de la personne concernée pour que la donnée soit considérée comme une donnée à caractère personnel. Selon un critère « relatif », de telles données doivent être considérées comme étant à caractère personnel seulement à l'égard de l'organisme en capacité de réidentifier la personne, et ne revêtent pas ce caractère à l'égard d'un autre organisme pour lequel l'identification nécessiterait des efforts démesurés. La Cour de justice avait retenu le critère « relatif » pour qualifier les adresses IP dynamiques comme des données à caractère personnel à l'égard du fournisseur, CJUE, 19 oct. 2016, *Patrick Breyer* c. *Bundesrepublik Deutschland*, C-582/14, § 31 s. V. *supra,* nº 189.
[994] *Dictionnaire de l'Académie française*, 9e éd., *Vº* « Objet », sens II.
[995] *Dictionnaire de l'Académie française*, 9e éd., *Vº* « Objectif », sens II.2.
[996] *Dictionnaire de l'Académie française*, 9e éd., *Vº* « Finalité », sens I.
[997] S. Guinchard et T. Debard (dir.), *Lexique des termes juridiques*, Dalloz, 2020, *Vº* « Objet », droit civil.
[998] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vº* « Objectif », sens 2.
[999] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vº* « Objectif », sens 1.

L'utilisation du terme objet dans le critère proposé renvoie directement à ces définitions. Lorsque le traitement opéré sur la donnée vise à faire un lien avec une personne, il doit être considéré comme ayant *pour objet* d'établir un tel lien. Ce critère fait donc entrer dans la notion de donnée à caractère personnel toutes les données dont les traitements cherchent à individualiser les personnes. Dans ce contexte, la donnée indirectement identifiante est alors qualifiée comme une donnée à caractère personnel.

Pour autant, il est impossible pour l'homme de sonder les cœurs ou les esprits[1000]. Le critère du traitement ayant « pour effet » permet justement de contourner cette difficulté.

276. Précisions concernant la référence au traitement ayant « pour effet ». Selon le dictionnaire de l'Académie française, le terme effet s'entend comme la « conséquence d'un acte, d'un phénomène »[1001]. En droit, ce terme fait référence à la conséquence d'une action ou d'une chose[1002]. Appliqué à la définition proposée, ce terme renvoie à l'idée que certains traitements conduisent le responsable du traitement, même sans le vouloir, à établir un lien entre la donnée et la personne. La référence à l'effet doit donc être entendu comme la conséquence, même involontaire, du traitement mis en œuvre par l'organisme. Ainsi, lorsque l'ensemble du traitement ou certains croisements de données aboutissent à l'établissement d'un lien entre la donnée et la personne, la donnée indirectement identifiante doit être considérée comme une donnée à caractère personnel.

Le caractère volontaire ou involontaire de l'établissement du lien entre la donnée et la personne est donc indifférent pour la qualification : ce qui importe, c'est le résultat auquel aboutit le traitement.

277. Précisions concernant la référence du « lien avec une personne physique ». Il semble essentiel de préciser ce qui doit être entendu par « établir un lien avec une personne physique ». Souvent, le processus d'identification a deux objectifs alternatifs : dans certains cas, le responsable du traitement souhaite établir un lien avec

---

[1000] Selon le livre de Jérémie, « Moi, Yahvé, je scrute le cœur, je sonde les reins pour donner à chacun selon sa conduite », Ancien Testament, *Livre de Jérémie*, Chapitre 17, 10.
[1001] *Dictionnaire de l'Académie française*, 9e éd., *Vo* « Effet », sens II.
[1002] Plus précisément, il s'agit de la « conséquence juridique résultant d'un acte juridique (effet obligatoire du contrat), d'un délit (responsabilité), d'une loi, d'une décision juridictionnelle ou administrative », G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vo* « Effet (I) ».

« l'identité stable » de la personne[1003], dans d'autres cas, il s'intéresse plutôt à sa présence[1004].

Établir un lien avec l'identité stable revient, en pratique, à rattacher la donnée indirectement identifiante à un ou plusieurs attributs permanents de la personne[1005]. Dans ce cas, le responsable du traitement cherche à connaître, grâce à l'information indirectement identifiante, le nom, le prénom ou un des attributs de la personne. C'est le cas, par exemple, d'un opérateur qui demande aux fournisseurs d'accès à Internet de révéler l'identité de l'abonné ayant utilisé une certaine adresse IP[1006]. Dans cette situation, la donnée indirectement identifiante (l'adresse IP) ne révèle l'identité de son utilisateur qu'à l'occasion d'un traitement particulier (le croisement effectué par le fournisseur d'accès à Internet). D'autres traitements peuvent être effectués afin de faire un lien avec la personne dans le but d'obtenir des informations relatives à sa présence.

Lorsque le responsable du traitement ne s'intéresse pas l'identité stable de la personne, il peut être intéressé par les éléments relatifs à sa présence[1007]. Une analyse de ces éléments peut l'aider à mieux l'influencer[1008], souvent avec l'objectif de lui faire accepter des propositions commerciales, politiques ou idéologiques[1009]. Pour ces traitements de données, le responsable du traitement cherche surtout à connaître les affinités, les goûts, les réactions, les cheminements de pensée de la personne… Dans cette quête, toutes les données sont utiles : le défilement plus ou moins complet de l'écran renseigne sur le degré d'intérêt de la personne pour le site visité, l'historique des déplacements renseigne sur ses habitudes[1010], l'analyse des emails dévoile ses

---

[1003] J. Rochfeld, *Les grandes notions du droit privé,* 2e éd., PUF, 2013, *Vo* « La personne », no 16, p. 39.
[1004] Sur la distinction entre l'identité stable et la présence, v. J. Rochfeld, « La vie tracée ou le code civil doit-il protéger la présence numérique des personnes ? », in *Mélanges J. Hauser*, LexisNexis et Dalloz, 2012, p. 619 s., no 4, spéc. p. 621 ; L. Merzeau, « La présence, plutôt que l'identité », *Documentaliste-Sciences de l'Information* 2010*,* vol. 47, p. 32 ; F. Bellivier, *Droit des personnes*, LGDJ, 2015, no 47, p. 65 s. Monsieur Emmanuel Netter distingue plusieurs types d'identité (stable, choisie, représentation et numérique), E. Netter, *Numérique et grandes notions du droit privé. La personne, la propriété, le contrat*, mémoire en vue de l'habilitation à diriger des recherches en droit privé, Picardie, 20 nov. 2017, nos 29 s., p. 47 s.
[1005] J. Carbonnier, *Droit civil,* vol. 1, *Introduction. Les personnes. La famille, l'enfant, le couple*, PUF, 2004, no 219, p. 419 s. ; G. Cornu, *Droit civil. Les personnes*, 13e éd., Montchrestien, 2007, nos 37 s., p. 83 s. V. aussi *supra*, no 112.
[1006] V. *supra,* no 187.
[1007] On peut également parler de personnalité numérique qui est « la projection – volontaire ou involontaire – de sa personnalité dans un environnement numérique », B. Gleize, « La personnalité numérique », in *Mélanges M. Vivant,* Dalloz, 2020, p. 189 s., spéc. p. 194.
[1008] Sur cette influence et ses risques pour les personnes, v. V. *infra*, no 387.
[1009] H. Le Crosnier, « La documentarisation des humains », *Documentaliste-Sciences de l'Information* 2010*,* vol. 47, p. 34.
[1010] S. Thompson et C. Warzel, « Twelve million phones, one dataset, zero privacy », *The New York Times* 19 déc. 2019. Certaines entreprises continuent de collecter ces informations même lorsque la personne concernée refuse explicitement, v. not. R. Nakashima, « Google tracks your movements, like it or not », *Associated Press* 14 août 2018. Pour éviter ces traçages intrusifs, des techniques de protection de données ont été mises en place, v. par ex. Apple, « Location services privacy overview. Learn how location services protects your privacy », nov. 2019.

intérêts et ses relations ainsi que leur fréquence[1011]… La liste de ces données est longue et ne cesse de s'étendre. Sur le modèle du pointillisme en peinture, les petites traces laissées sur la toile offrent, dans une amélioration perpétuelle de l'œuvre[1012], un portrait de plus en plus réel et détaillé de la personne. Dans ce modèle, le responsable du traitement n'identifie pas la personne au sens classique du terme. Il cherche plutôt à la classer dans une ou plusieurs catégories : tranche d'âge, catégorie socio-professionnelle, caractère dépensier ou économe[1013]... Même si le responsable du traitement ne souhaite pas connaître le nom ou prénom de la personne, il cherche tout de même à la faire entrer dans certaines catégories afin de la distinguer des autres utilisateurs.

Ainsi, même si ces processus d'identification visent à percevoir la personne de manière différente (dans un cas il s'agit d'identifier la personne au sens classique, dans l'autre il s'agit de l'identifier dans un sens plus moderne), ces traitements doivent être considérés comme établissant « un lien avec une personne physique ».

278. Définition extensive de la notion de traitement en droit positif. La notion de traitement est définie largement dans le droit positif puisqu'il s'agit de « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »[1014]. La liste d'exemples est évidemment non exhaustive et a pour objectif principal de souligner la polysémie du terme qui s'entend à la fois comme un acte positif ou comme une inertie[1015]. L'interprétation retenue par les interprètes de cette

---

[1011] E. Andrieu, « Internet et la protection des données personnelles », *Legicom* 2000, n° 21-22, p. 155, spéc. p. 162.
[1012] La collecte des données est continue, c'est-à-dire que toute activité, même la plus triviale, est enregistrée et traduite en données.
[1013] D'ailleurs, avec sa fonctionnalité « pourquoi est-ce que je vois ca ? », Facebook montre la variété des catégories utilisées pour regrouper les personnes, v. Facebook, « Facebook lance la fonctionnalité "Pourquoi est-ce que je vois ça ?" dans le fil d'actualité », *About.fb.com* 1 avr. 2019.
[1014] Art. 4 § 2 du règlement UE n° 2016/679. Pour une analyse détaillée de cette notion, v. O. Tambou, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, n^{os} 80 s., p. 72 s. ; M. Bourgeois, *Droit de la donnée. Principes théoriques et approche pratique,* LexisNexis, 2017, n^{os} 122 s., p. 37 s.
[1015] N. Martial-Braz et J. Rochfeld (dir.), *Droit des données personnelles. Les spécificités du droit français au regard du RGPD,* Dalloz, 2019, n° 206, p. 35. V. déjà sur cette accumulation des termes, A. Lucas, J. Devèze et J. Frayssinet, *Droit de l'informatique et de l'Internet*, PUF, 2001, n° 112, p. 82.

notion est évidemment très large[1016]. Ainsi, l'expression de traitement telle qu'elle est définie par le droit des données à caractère personnel et interprétée permet d'éviter d'éventuelles stratégies de contournement.

SOUS-SECTION II – BÉNÉFICES DE LA PROPOSITION

279. Plan. La proposition de critère de qualification des données indirectement identifiantes formulée, il convient désormais de s'interroger sur ses avantages et ses éventuels risques. Ce critère encadre-t-il avec justesse la notion, tout en assurant une protection cohérente des personnes ? Ne risque-t-il pas d'exclure trop de données du domaine des données à caractère personnel ? Après avoir démontré la cohérence résultant de cette nouvelle définition (§ I), nous verrons que celle-ci s'inscrit dans la logique actuelle du droit des données à caractère personnel (§II).

§ I. Une protection cohérente des données

280. Une définition adaptée aux traitements. D'intenses débats ont eu lieu sur la qualification juridique de données indirectement identifiantes. Par exemple, la qualification de l'adresse IP ou des métadonnées a été difficile à trancher parce qu'il est compliqué d'affirmer qu'une suite de chiffre ou une heure peuvent être qualifiés de donnée à caractère personnel. Pourtant, certains des traitements effectués sur ces informations d'apparence triviale engendrent d'importantes implications pour les personnes[1017]. Ainsi, ce n'est pas la donnée prise en tant que telle qui renseigne sur la personne, mais plutôt le traitement effectué sur celle-ci.

[1016] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, n^os^ 446 s., p. 196. Pour une analyse de l'application de la notion, v. not. V.-L. Benabou, « L'extension du domaine de la donnée », *Légicom* 2017, n^o^ 59, p. 3, spéc. p. 6 s.

[1017] La Cour de justice de l'Union européenne considère que les traitements de données indirectement identifiantes (telles que les données relatives au trafic) peuvent être plus dangereux pour la vie privée que ceux relatifs aux données de l'identité civile des utilisateurs. En effet, la Cour a affirmé « qu'en ce qui concerne les données relatives à l'identité civile des utilisateurs des moyens de communications électroniques, ces données ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires des communications effectuées, non plus que les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée, de telle sorte qu'elles ne fournissent, mises à part les coordonnées de ceux-ci, telles que leurs adresses, aucune information sur les communications données et, par voie de conséquence, sur leur vie privée. Ainsi, l'ingérence que comporte une conservation de ces données ne saurait, en principe, être qualifiée de grave », CJUE, 6 oct. 2020, *La Quadrature du Net* c. *Premier ministre*, C-511/18, C-512/18 et C-520/18, § 157.

281. Les bénéfices de l'approche téléologique. En retenant une qualification téléologique, plutôt qu'une qualification *in abstracto,* le critère proposé permet à la notion de retrouver une cohérence d'ensemble. La donnée à caractère personnel est celle ayant un rapport avec une personne.

D'un côté, la notion continue d'accueillir les données liées aux personnes, c'est-à-dire celle identifiantes par nature et celles dont le traitement établit une identification. De l'autre, la notion ne s'étend pas de manière indue à des informations éloignées des personnes et sur lesquelles aucun traitement d'identification n'est effectué. Ce critère permet de garantir la libre circulation des données indirectement identifiantes, favorisant ainsi les libertés d'information et d'expression.

À ce titre, l'absence de conséquence de l'ouverture, en *open data,* de certaines bases de données indirectement identifiantes prouve que les risques d'atteinte aux personnes sont souvent très relatifs pour les données indirectement identifiantes. Cette approche renforce donc la protection des droits des personnes en trouvant un équilibre entre la protection des données personnelles et les principes de libre circulation de l'information : elle protège les personnes contre les traitements de leurs données, tout en reconnaissant la possibilité d'établir des statistiques générales ou d'effectuer des traitements anodins ou sans risque pour les personnes[1018]. Le nouveau critère de définition permet donc de surmonter les difficultés de qualification de certaines données très indirectement identifiantes et encadre l'expansion du domaine de la donnée à caractère personnel.

282. L'efficacité de l'approche téléologique. De nombreux secteurs d'activité collectent des données indirectement identifiantes pour des finalités diverses. Par exemple, les entreprises spécialisées dans la publicité ciblée collectent de nombreuses données indirectement identifiantes telles que les adresses IP, les types et numéros de terminaux, les sites visités, les heures de connexion et ce, dans le but d'établir des profils d'utilisateurs. Souvent, ces entreprises se défendent de collecter des données à caractère personnel, alors même qu'elles reconnaissent chercher à *personnaliser* leurs

[1018] À ce titre, la CNIL opère d'ailleurs une distinction entre les traceurs nécessaires à la fourniture du service et les autres, v. CNIL, délibération nº 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération nº 2019-093 du 4 juillet 2019, § 50 s.

services[1019]. Il est vrai que le droit a longtemps laissé planer un doute sur la qualification des données traitées par ces secteurs d'activité[1020]. L'approche téléologique clarifie le statut de ces traitements. Lorsque la collecte de données *vise* à distinguer des personnes pour les tracer dans leurs activités, ce traitement relève, sans conteste, du nouveau critère. Ce critère téléologique évite donc une application trop large de la notion de donnée à caractère personnel, tout en garantissant une protection de ces données.

283. Une approche liée aux effets des traitements. En ciblant la protection sur les traitements effectifs de données plutôt que sur la capacité abstraite des données à faire un lien avec la personne, ce nouveau système encourage les responsables du traitement à s'intéresser aux effets de leurs traitements. Il les incite donc à adopter une logique appropriée aux risques générés par leurs traitements. Cette logique est au cœur du règlement européen.

§ II. Une approche conforme à la logique actuelle du droit des données à caractère personnel

284. La logique de responsabilité du règlement. En favorisant une application de la notion *in concreto,* la nouvelle définition s'inscrit dans la logique de responsabilisation des organismes, laquelle a été érigée comme principe cardinal du droit des données à caractère personnel[1021]. En effet, la plupart des obligations de ce droit encouragent les responsables du traitement à s'intéresser aux traitements et à leurs conséquences pour les individus[1022]. Par exemple, l'obligation de tenir un registre indiquant les traitements et leurs finalités contraint les responsables du traitement à s'intéresser aux effets de leurs traitements, notamment parce qu'ils doivent s'assurer de la pertinence des données collectées[1023]. L'obligation de mener une analyse d'impact relative à la protection des données est une autre illustration de la logique actuelle du

[1019] J. Rochfeld, « La vie tracée ou le code civil doit-il protéger la présence numérique des personnes ? », in *Mélanges J. Hauser*, LexisNexis et Dalloz, 2012, p. 619 s., nº 11, spéc. p. 631.
[1020] Les débats sur la qualification de l'adresse IP comme donnée à caractère personnel illustrent bien ces difficultés, v. *supra*, nºs 186 s.
[1021] V. *infra*, nº 314.
[1022] Sur l'évolution du régime, v. not. K. Favro, « La démarche de *compliance* ou la mise en œuvre d'une approche inversée », *Légicom* 2017, nº 59, p. 21.
[1023] Art. 30 du règlement UE nº 2016/679.

droit des données à caractère personnel[1024]. En effet, pour savoir si le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, encore faut-il que le responsable du traitement connaisse et comprenne les conséquences de ses traitements[1025]. La nouvelle définition de la donnée à caractère personnel encourage les responsables du traitement à analyser, avant leur mise en œuvre, les conséquences de leurs traitements, puisque c'est grâce à cette détermination qu'ils savent quel est le régime applicable aux données qu'ils traitent.

285. Des risques liés au nouveau critère ? Certaines critiques pourraient être formulées à l'égard du critère proposé. D'aucuns pourraient considérer qu'une telle approche donne trop de pouvoir aux responsables du traitement quant à la détermination des données qui doivent, ou non, relever de la notion de donnée à caractère personnel. En effet, cette approche pourrait aboutir à une appréciation subjective de la notion octroyée aux responsables du traitement. Cette définition leur accorderait un pouvoir démesuré, au détriment des personnes concernées qui se verraient imposer une qualification qu'elles auraient sans doute du mal à contester par la suite puisque seuls les responsables du traitement peuvent connaître l'impact des technologies qu'ils développent[1026]. Ces critiques, bien que parfaitement recevables, doivent être tempérées notamment parce que le système actuel peut être soumis au même reproche. En effet, la détermination de la qualification des données traitées relève d'ores et déjà de la compétence du responsable du traitement. D'ailleurs, dans plusieurs affaires, la CNIL et les tribunaux ont requalifié des données qui n'avaient pas été considérées comme des données à caractère personnel par les responsables du traitement[1027]. La nouvelle définition devra donc s'accompagner d'une augmentation

[1024] En vertu de l'article 35 du règlement UE nº 2016/679, cette analyse d'impact relative à la protection des données impose au responsable du traitement de faire, préalablement au traitement, une analyse de l'impact des opérations envisagées sur la protection des données à caractère personnel. Elle est obligatoire pour les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, v. CNIL, « Analyse d'impact relative à la protection des données : publication d'une liste des traitements pour lesquels une analyse est requise », 6 nov. 2019, et CNIL, « Analyse d'impact relative à la protection des données : publication d'une liste des traitements pour lesquels une analyse n'est pas requise », 22 oct. 2019.

[1025] Des auteurs ont tenté de cerner les contours de la notion de risque en droit des données personnelles, v. par ex., R. Gellert, *The risk-based approach to data protection*, Oxford University Press, 2020 ; R. Gellert, « Understanding the notion of risk in the general data protection regulation », *Computer Law & Security Review* 2018, vol. 34, nº 2, p. 279.

[1026] Le déséquilibre informationnel est inhérent aux traitements de données à caractère personnel. Pour pallier ces difficultés, le législateur a organisé des obligations d'information à la charge des organismes, v. *infra*, nº 548.

[1027] V. par ex., Cass. civ. 1re, 3 nov. 2016, nº 15-22.595, *Bull. civ.* 2016, nº 206, p. 251.

des contrôles et d'une plus grande sévérité dans les sanctions prononcées en cas de manquement[1028].

D'autres critiques pourraient considérer que cette protection risque de permettre à des tiers peu scrupuleux de traiter des données indirectement identifiantes sans égard pour les personnes concernées. Ici encore, cette observation peut être adressée à tous les systèmes aménageant la permission de traiter des données à caractère personnel[1029], y compris le système actuel. En effet, comme les traitements des données personnelles sont permis, le contrôle de la conformité de ces traitements ne peut se faire qu'*a posteriori*[1030].

Le critère proposé répond donc aux besoins d'encadrement identifiés.

286. Conclusion de chapitre. Des propositions de redéfinition de la notion de donnée à caractère personnel ont été formulées par la doctrine. Si ces propositions présentent des analyses intéressantes, notamment parce qu'elles tentent de mieux protéger les personnes, aucune d'entre elles ne répond aux risques identifiés d'une application trop étendue de la notion de donnée à caractère personnel. Seule la proposition de Madame Helen Nissenbaum, qui s'intéresse au contexte dans lequel la donnée circule, propose de retenir une approche centrée autour du traitement. Toutefois, son application au droit européen semble peu adaptée.

L'approche proposée s'inspire des travaux doctrinaux antérieurs et s'inscrit profondément dans la notion actuelle de donnée à caractère personnel. Elle reprend la distinction classique entre les données directement identifiantes et les données indirectement identifiantes. Seule cette dernière catégorie de données est modifiée. Pour ces données, une approche téléologique, c'est-à-dire liée aux traitements, est retenue. Le nouveau critère prévoit donc que lorsque le traitement d'une donnée indirectement identifiante *a pour objet ou pour effet d'établir un lien avec une personne* elle doit recevoir la qualification de donnée à caractère personnel. Ce critère favorise une meilleure protection des personnes puisque les données trop éloignées des personnes peuvent toujours circuler librement et les données liées aux personnes sont protégées. Une protection effective des personnes est donc trouvée.

[1028] V. *infra*, n° 320.
[1029] Sur ce sujet, v. N. Ochoa, *Le droit des données personnelles, une police administrative spéciale*, th. Paris I, 2014, p. 73 s.
[1030] Sur le besoin d'amélioration des contrôles dans ce domaine, v. *infra,* n^os^ 463 s.

287. Conclusion de titre. L'expansion de la notion de donnée à caractère personnel est loin d'être neutre pour la protection des personnes et de leurs libertés. En ce qui concerne la vie privée d'abord, cette expansion n'a pas les effets escomptés. Au contraire, elle a tendance à banaliser les atteintes aux personnes en les diluant dans des immenses masses de traitements de données, sans que les effets réels sur les personnes ne soient pris en compte. En ce qui concerne les autres libertés, l'expansion de la notion se révèle avoir des effets négatifs. En s'appliquant de plus en plus largement, la notion de donnée à caractère personnel restreint les capacités d'information et d'expression des personnes.

Fondée sur l'objectif d'apporter une meilleure protection des personnes, une nouvelle définition de la donnée à caractère personnel a été recherchée. L'analyse des travaux doctrinaux montre que les définitions proposées répondent partiellement aux effets négatifs identifiés. Face à ces difficultés, il a semblé nécessaire de formuler une nouvelle proposition de définition. Celle-ci repose sur une approche téléologique et se limite aux données indirectement identifiantes, puisque c'est surtout pour celles-ci que l'expansion de la notion paraît démesurée. Les données directement identifiantes continuent, quant à elles, d'entrer automatiquement dans la notion. Le critère proposé reconnaît l'application de la notion aux données indirectement identifiantes lorsque leur traitement a *pour objet ou pour effet de faire un lien avec une personne physique*. Un tel critère donne une meilleure cohérence à la protection d'ensemble qui ressort du droit des données à caractère personnel.

CONCLUSION DE LA PREMIÈRE PARTIE

288. Depuis l'adoption des premières règles relatives aux données personnelles, le domaine des données à caractère personnel poursuit un mouvement d'expansion. Celui-ci s'illustre par l'activité prolifique des législateurs français et européen qui utilisent des termes extensifs pour la définir. Ce mouvement se retrouve aussi dans l'activité interprétative puisque les autorités de contrôle ont intégré de plus en plus d'informations dans le giron de leur compétence, tant et si bien qu'aujourd'hui, il est possible de se demander s'il existe encore des données non personnelles. Si les juridictions ont initialement fait preuve d'une plus grande prudence dans l'interprétation de la notion et n'ont reconnu le caractère personnel qu'aux données dont le lien avec la personne était incontestable, cette réserve s'est dissipée et les juridictions contribuent désormais activement à l'extension du domaine.

L'expansion de la notion a des effets sur la protection des personnes. Elle n'apporte pas les bénéfices escomptés, ni pour la protection de la vie privée, ni pour les autres libertés individuelles. Confronté à ces constats, une proposition d'encadrement a dû être formulée. Celle-ci vise à cibler la protection des données et à rendre la notion plus cohérente en restreignant son application aux seules informations dont le lien avec la personne n'est pas purement théorique. Reprenant le balancement classique entre les données directement et indirectement identifiantes, la définition retient une approche téléologique pour ces dernières. Si la donnée directement identifiante entre naturellement dans la notion de donnée à caractère personnel, la donnée indirectement identifiante a un critère d'application supplémentaire. Elle se voit reconnaître ce qualificatif lorsque le traitement effectué sur elle a pour objet ou pour effet de faire un lien avec une personne physique. Ainsi appréhendée, la notion de donnée à caractère personnel est encadrée de manière efficace et les personnes sont mieux protégées. Cette nouvelle définition appelle au renforcement du régime de protection de ces données.

DEUXIÈME PARTIE – RENFORCER LE RÉGIME DES DONNÉES À CARACTÈRE PERSONNEL

289. Le développement de la protection des droits de la personnalité. Au lendemain des atrocités perpétrées pendant la Seconde Guerre mondiale, les États ont souhaité instaurer un nouvel ordre international. Ils ont ainsi adopté de nombreux textes et mis en place des instances pour garantir les droits de l'Homme et les libertés individuelles[1031]. La protection de la personne humaine est apparue, plus que jamais, nécessaire dans ces sociétés déchirées et meurtries. L'individu, longtemps sacrifié sur l'autel de l'unité de la nation, y trouve une place renouvelée[1032]. En témoignent notamment les nombreuses déclarations internationales des droits et libertés[1033].

Dans le sillon de ces textes, les droits de la personnalité ont été consacrés dans plusieurs pays et notamment en France. Cette reconnaissance est née de la volonté du législateur de garantir aux personnes physiques une protection contre les atteintes dont elles pouvaient faire l'objet dans les différents aspects de leur personnalité[1034]. Elle est le témoin de la revalorisation de la personne, envisagée à la fois comme un individu irréductible à autrui et comme un membre du genre humain[1035]. En France, la consécration du droit au respect de la vie privée en 1970, puis celle du droit des données personnelles à la fin de cette même décennie, sont les témoins de cette revalorisation de la personne.

[1031] J.-P. Costa, *La Cour européenne des droits de l'homme. Des juges pour la liberté,* 2e éd., Dalloz, 2017, p. 20 s. Sur le développement d'une protection transnationale des droits fondamentaux, particulièrement à l'échelle européenne, v. not. L. Favoreu *et al.*, *Droit des libertés fondamentales*, 7e éd., Dalloz, 2015, nos 518 s., p. 455 s.
[1032] Il existe encore des sociétés dans lesquelles le nationalisme sacrifie toujours les libertés individuelles au profit de l'intérêt de la nation. En Chine par exemple, la répression visant les minorités musulmanes, notamment les Ouïghours, est fondée sur la vision selon laquelle la liberté de l'individu doit s'effacer au profit de l'intérêt collectif. Sont ainsi mises en place des collectes massives de données, notamment avec le crédit social, pour surveiller, puis arrêter et détenir ces populations, v. F. Lafargue, « Le "crédit social" ou le Big Brother à la sauce chinoise », *The Conversation* 20 juin 2018. V. aussi les travaux de l'association Human Rights Watch, v. not. Human Rights Watch, « Chine : collecte de l'ADN de millions d'habitants du Xinjiang. Des données personnelles sont recueillies par la police sous prétexte d'un programme de santé publique », 13 déc. 2017.
[1033] V. *supra*, no 5.
[1034] P. Jourdain, « Les droits de la personnalité à la recherche d'un modèle : la responsabilité civile », *Gaz. Pal.* 2007, no 139, p. 52.
[1035] *Rép. civ.* Dalloz, *Vo* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), no 19.

290. Une protection en phase avec les développements techniques L'une des spécificités du droit des données personnelles est son objet : ce droit se propose d'encadrer les développements de l'informatique[1036] pour que celle-ci reste respectueuse des individus[1037]. Depuis son origine, ce droit met donc en balance au moins deux intérêts : les développements de l'informatique et la protection de la personne. Cette balance est-elle toujours à l'équilibre ? L'un de ces deux intérêts n'a-t-il pas tendance à prévaloir sur l'autre dans une société de plus en plus dématérialisée ? L'équilibre recherché est délicat puisqu'il doit prendre en compte les attentes sociales, caractérisées notamment par un renouvellement des formes d'exposition de soi[1038], mais aussi les intérêts des organismes traitant des données personnelles. La protection qui en résulte est nécessairement relative, puisqu'elle oscille entre des intérêts divergents, voire contradictoires[1039].

291. Des évolutions constantes. Après seulement quatre décennies d'existence, le droit des données à caractère personnel a d'ores et déjà fait l'objet de plusieurs réformes d'ampleur. Ces aménagements sont apparus nécessaires pour garantir l'effectivité de ses principes. Il est vrai que, dans une matière aussi nouvelle et dépendante des développements technologiques, et à défaut de maxime générale, l'adaptabilité doit être le maître mot.

La réforme du droit européen des données à caractère personnel, entrée en application en 2018, symbolise particulièrement bien ces rééquilibrages. Cette réforme acte le passage d'une logique de formalité préalable à une logique de conformité continue, avec une baisse du contrôle *a priori*[1040], et mise sur le renforcement de la régulation tant par les responsables du traitement que par les autorités de protection[1041]. Face à ces évolutions, il convient de se demander si le droit positif répond à l'ensemble

---

[1036] L'informatique doit ici être entendue comme la « science du traitement rationnel et automatique de l'information ; l'ensemble des applications de cette science », *Dictionnaire de l'Académie française*, 9e éd., *Vo* « Informatique », sens 1.
[1037] Pour éviter des stratégies de contournement, les fichiers non automatisés entraient, le plus souvent, dans le champ d'application de ce droit.
[1038] Sur des analyses sociologiques de l'exposition de soi, v. F. Granjon et J. Denouël, « Exposition de soi et reconnaissance de singularités subjectives sur les sites de réseaux sociaux », *Sociologie* 2010, vol. 1, p. 25.
[1039] Selon Messieurs André Lucas, Jean Devèze et Jean Frayssinet, le droit des données personnelles tend « à établir les règles du jeu, à établir des équilibres entre des aspirations et intérêts différents, concurrents, parfois contradictoires, dans une société ouverte, démocratique, libre », A. Lucas, J. Devèze et J. Frayssinet, *Droit de l'informatique et de l'Internet*, PUF, 2001, no 2, p. 2.
[1040] J. Antippas et B. Beignier, « La protection de la vie privée », in *Libertés et droits fondamentaux 2020*, R. Cabrillac (dir.), 26e éd., Dalloz, 2020, no 275, p. 233.
[1041] O. Tambou, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, no 14, p. 9.

des atteintes aux personnes permises par les traitements de données. Dans le cas contraire, certains ajustements ne peuvent-ils pas être proposés ?

292. Le renforcement de la mise en œuvre. La logique de responsabilité des organismes a renforcé leurs pouvoirs en ce qui concerne la mise en œuvre concrète de la protection des personnes[1042]. Corrélativement, et pour contrebalancer les risques inhérents à cette responsabilisation, le dispositif de sanction a été renforcé. Il apparaît nécessaire de s'assurer que les contrôles sont suffisamment nombreux et diversifiés pour garantir une mise en œuvre effective du droit des données à caractère personnel. À cet égard, il faut sonder la réalité de la mise en œuvre de cette matière pour savoir si celle-ci est effective ou si elle a plutôt tendance à être théorique ou illusoire. Dans cette perspective, les rôles et places de l'autorité de contrôle, des experts en données, des associations et du juge devront être étudiés afin de vérifier que tous les acteurs contribuent efficacement à la protection des personnes.

293. Plan. La complexité apparente du régime des données à caractère personnel a tendance à effacer un facteur pourtant essentiel de ce droit : ses règles sont favorables aux traitements de données. La protection des personnes qui en résultent est donc relative, et une consolidation des règles de protection semble nécessaire (Titre I). Pour sonder l'effectivité de la protection des personnes résultant de ces règles, il conviendra ensuite de s'intéresser à leur mise en œuvre et, le cas échéant, d'en proposer une amélioration (Titre II).

[1042] C. Scottez, « Le RGPD, un nouveau paradigme de la protection des données personnelles pour les professionnels et le régulateur », *Dalloz IP/IT* 2019, p. 229.

TITRE I – CONSOLIDER LES RÈGLES DE PROTECTION DES PERSONNES

294. Des règles perfectibles. Le droit des données personnelles navigue entre des intérêts variés. Si la protection de ces données en est le fil rouge, d'autres intérêts viennent souvent empiéter sur son domaine : liberté d'innovation, droit à la preuve, numérisation de la société, *open data*, enquêtes journalistiques, liberté d'expression, etc. De nombreux exemples témoignent de la variété des intérêts pris en compte dans le droit des données à caractère personnel. Par exemple, l'entreprise qui vieillit l'image d'un visage à partir de photographies souhaite surtout améliorer son algorithme de reconnaissance faciale[1043] ; ou le journaliste qui épluche l'agenda d'un ministre veut montrer le rôle des lobbys dans la prise de décision politique[1044]. À cette variété d'intérêts pris en compte par le droit des données à caractère personnel s'ajoutent également les risques liés aux traitements de ces données particulières. Longtemps, les atteintes aux personnes se limitaient aux risques liés à la divulgation d'informations ou à leur centralisation. Aujourd'hui, ces atteintes ont évolué et le droit peine parfois à répondre aux nouvelles formes de manipulation permises par les traitements de données. Ces facteurs témoignent d'une protection relative des personnes par le droit des données à caractère personnel.

295. Des évolutions nécessaires. Parmi les nombreux principes du droit des données à caractère personnel, certains ont des effets importants sur la protection des personnes. Par exemple, quelle est la place de la liberté d'expression dans la reconnaissance du droit à l'oubli ? Ou encore, quel pouvoir de contrôle reste-t-il aux personnes dont les données sont transférées à une multitude de tiers ? Pour garantir une meilleure protection des personnes, certains des principes du droit des données doivent évoluer.

[1043] M. Szadkowski, « FaceApp : pourquoi il faut se méfier de l'application et de son filtre à selfie pour se voir vieux », *Le Monde* 17 juill. 2019.
[1044] Actuellement, ces agendas sont très incomplets et les formats des données empêchent une exploitation facile des informations, v. X. Berne, « Mesdames, messieurs les ministres, pourriez-vous publier vos agendas en open data ? », *NextInpact* 2 juill. 2018.

296. Plan. Après avoir constaté que le droit des données personnelles apporte une protection relative de la personne (Chapitre I), nous proposerons des ajustements de certains principes, dans l'objectif de renforcer cette protection (Chapitre II).

Chapitre I – Droit positif : une protection relative des personnes par le droit des données à caractère personnel

297. La diversité d'intérêts en présence. Jusque dans leurs titres, les textes européens rappellent l'importance de deux objectifs primordiaux de ce droit : la *protection* des données et leur *libre circulation* sur le territoire européen[1045]. Contrairement à une impression communément admise, la seule conformité aux formalités préalables, lorsqu'elles étaient applicables, ne suffisait pas à rendre licites les traitements de données. Cette déclaration constituait la première étape d'un ensemble plus large de règles relatives à la collecte, à l'enregistrement, aux opérations et à la conservation des informations nominatives. Ces règles, reprises par le droit positif, incluaient des principes de pertinence, de conservation limitée, de sécurité, et reconnaissaient des droits aux personnes concernées. Pour résumer, le droit des données personnelles vise à encadrer, dans le temps, dans l'espace et dans ses effets, l'atteinte portée à l'individu par l'utilisation de ses données.

Une opinion doctrinale a même été jusqu'à affirmer que le droit des données à caractère personnel n'était pas destiné à protéger « les droits et libertés de la personne fichée, mais la liberté informatique elle-même »[1046]. En effet, selon cette opinion, la loi Informatique et libertés aurait consacré la liberté de chacun d'utiliser des procédés informatiques, dont la limite serait le respect des droits fondamentaux des personnes physiques[1047]. Sans aller jusqu'à une telle affirmation, il est possible de constater que le droit des données personnelles a une double finalité : il organise les conditions de licéité des atteintes aux personnes concernées et leur accorde, en contrepartie, une série de droits. Comment le droit des données à caractère personnel réussit-il à trouver un équilibre entre ces deux intérêts apparemment contradictoires ? La recherche de cet équilibre amène à s'interroger sur l'étendue de la protection accordée par ce droit. Plus précisément, il est opportun de se demander si le droit positif répond effectivement à l'ensemble des atteintes aux personnes engendrées par les traitements des données à caractère personnel.

[1045] D'ailleurs, le principe de libre circulation des données apparaît désormais comme une véritable liberté de circulation, v. I. Boev, « Le nouveau règlement : un 5e principe de libre circulation ? », *Dalloz IP/IT* 2020, p. 223. Ce principe ne s'applique pas au-delà des frontières européennes puisque, pour ces transferts de données, le principe est justement l'interdiction, v. art. 44 s. du règlement UE n° 2016/679. D'ailleurs, les transferts de données vers les États-Unis, notamment sur le fondement des décisions d'adéquation et des clauses contractuelles types, ont été plusieurs fois remis en cause, v. *supra*, n° 19.

[1046] N. Ochoa, *Le droit des données personnelles, une police administrative spéciale*, th. Paris I, 2014, p. 202.

[1047] N. Ochoa, *Le droit des données personnelles, une police administrative spéciale*, th. Paris I, 2014, p. 203.

298. Plan. L'une des principales caractéristiques du droit des données à caractère personnel est qu'il organise les traitements de ces données (Section I). En pratique, les traitements présentent des risques d'atteinte aux personnes (Section II).

SECTION I – DES RÈGLES PERMETTANT LES TRAITEMENTS

299. Rappel de la définition de la donnée à caractère personnel. Pour éviter une application trop étendue du domaine des données à caractère personnel, une approche téléologique a été proposée pour les données indirectement identifiantes. Celle-ci invite les organismes à s'intéresser aux traitements qu'ils mettent en œuvre afin de déterminer si un lien avec la personne est susceptible de se manifester du fait de ces traitements. Le critère principal de cette notion est donc fondé sur les *effets du traitement*, lesquels déclenchent, éventuellement, l'application du régime des données personnelles.

300. Principe. L'objectif du droit des données personnelles a toujours été de « maîtriser et non paralyser l'informatique »[1048]. C'est sans doute ce qui explique qu'avant toute chose, ce droit organise les modalités de licéité des traitements de données et n'a pas pour but de les empêcher. Par principe donc, tant qu'ils respectent certaines règles, les traitements de données sont permis[1049]. Ces règles ont souvent une réputation négative auprès des responsables du traitement qui les considèrent comme une charge importante, sans voir de réelle contrepartie. Une étude de ces règles montre qu'elles sont plutôt accommandantes et permissives. La protection de la personne en résultant est donc relative.

301. Évolutions de la matière. La réforme de 2016 a considérablement allégé le système déclaratif au profit d'autres logiques de protection. Ces dernières étaient déjà à l'œuvre dans diverses branches du droit (notamment en droit bancaire et financier), et s'inspirent de certains modèles de régulation mis en œuvre aux États-Unis.

[1048] B. Tricot, « Rapport de la commission Informatique et libertés », La Documentation française, 1975, p. 23.
[1049] L'article 9 du règlement UE nº 2016/679 interdit, en principe, 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 l'orientation sexuelle d'une personne physique ». Toutefois, le nombre d'exceptions légitimant le traitement de ces données remet en cause, au moins partiellement, ce principe d'interdiction. Pour une étude relative aux traitements de données sensibles et le caractère symbolique du principe d'interdiction, v. C. Koumpli, *Les données personnelles sensibles. Contribution à l'évolution du droit fondamental à la protection des données à caractère personnel*, th. Paris I, 2019, p. 432 s.

Documentation, mise en conformité, *compliance*, responsabilisation des acteurs, corégulation sont les maîtres-mots de cette matière renouvelée[1050]. En plus de cette modification substantielle, d'autres évolutions, plus modérées, ont également été adoptées. Par exemple, sous une apparente continuité, les conditions de licéité des traitements de données ont été ajustées. L'ensemble de ces modifications témoignent de l'augmentation de la confiance accordée aux responsables du traitement. Plutôt que de réduire les traitements de données effectués, ces évolutions sont favorables à leur mise en œuvre.

302. Plan. Les règles issues du règlement européen ont largement refondé le système déclaratif. Un tel changement renverse le paradigme jusqu'alors à l'œuvre dans cette matière (Sous-section I). Le nouveau régime propose toujours une pluralité de fondements juridiques permettant aux responsables du traitement de mettre en œuvre leurs traitements (Sous-section II).

SOUS-SECTION I – L'ASSOUPLISSEMENT DU RÉGIME DÉCLARATIF

303. Plan. La logique sur laquelle reposaient les premières règles du droit des données personnelles visait principalement à anticiper les atteintes aux personnes. Le régime était donc principalement préventif (§ I). Cette logique a récemment évolué vers un régime répressif rapprochant le droit des données à caractère personnel du droit au respect de la vie privée (§ II).

§ I. L'existence d'un régime historiquement préventif

304. La genèse des règles en matière de données personnelles. L'apparition généralisée des ordinateurs et le développement du numérique et d'Internet ont modifié en profondeur la relation entretenue par les personnes à l'égard de l'information. Dès les années 1960, certains commentateurs se sont interrogés sur les implications de ces développements sur les libertés individuelles et ont appelé les législateurs à intervenir afin d'éviter la réalisation de ces risques[1051]. Plusieurs scandales tels que le Watergate aux États-Unis, l'affaire des plombiers en France ou encore les projets

[1050] B. Fauvarque-Cosson et W. Maxwell, « Protection des données personnelles », *D.* 2018, p. 1033.
[1051] A. Westin, *Privacy and Freedom*, Ig Publishing, 1968, réimpr. 2015, p. 334.

gouvernementaux visant à regrouper des dizaines de fichiers en un seul fichier, ont confirmé le besoin d'adopter des principes législatifs pour protéger les informations personnelles[1052].

Une brève période de convergence a existé entre les réponses juridiques européennes et américaines, matérialisée notamment par la diffusion des principes du *code of fair information practices*. Ce code, issu d'un rapport américain de 1973, encourageait l'adhésion à plusieurs principes[1053] :

- l'interdiction de collecter des données personnelles de manière secrète (principe de transparence),
- l'existence d'un moyen pour la personne concernée de connaître les informations détenues par un organisme et leurs utilisations (droit d'accès),
- l'existence d'un moyen pour la personne concernée d'empêcher que les données collectées pour un but donné ne soient utilisées ou mises à disposition pour d'autres finalités (principe de finalité et d'opposition),
- l'existence d'un moyen pour la personne concernée de corriger ou modifier ses données personnelles (principe de rectification et de modification),
- l'obligation pour tout organisme créant, maintenant, utilisant ou diffusant des dossiers et des données personnelles d'assurer la fiabilité de ces informations pour l'usage auquel elles sont destinées et de prendre les précautions nécessaires pour empêcher leur détournement (principe de sécurité et principe de finalité).

Ces principes ont servi de base aux travaux législatifs postérieurs puisqu'ils se retrouvent dans de nombreux textes nationaux et internationaux[1054]. Ces principes

---

[1052] Sur ces scandales, v. *supra*, nº 174.

[1053] Ces principes sont présentés dès les premières pages du rapport. Ils prévoient que « There must be no personal data record-keeping systems whose very existence is secret. There must be a way for a person to find out what information about the person is in a record and how it is used. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent. There must be a way for a person to correct or amend a record of identifiable information about the person. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data », pouvant être traduit comme : « Il ne doit pas exister de base de données personnelles dont l'existence serait secrète. La personne doit avoir un moyen de savoir quelles informations sont présentes dans la base de données et comment elles sont utilisées. La personne doit pouvoir empêcher que des données collectées pour un objectif soient utilisées ou mises à disposition pour d'autres objectifs sans son consentement. Il doit être prévu une façon pour la personne de rectifier, de modifier un document contenant des informations identifiantes à propos d'elle. Toute organisation créant, maintenant, utilisant ou disséminant des bases de données doit s'assurer de la fiabilité des données et doit s'assurer de prévenir les mauvais usages des données. », v. United States Department of Health, Education and Welfare, « Records, computers, and the rights of citizens », 1973, p. xxiiii.

[1054] D. Lindsay, « The relationship between general law protection of privacy and information privacy laws », in A. Saad, *Personal data & privacy protection*, LexisNexis, 2005, p. 29.

demeurent, encore aujourd'hui, des conditions essentielles de la protection juridique des données.

305. Les principes de la loi Informatique et libertés. En France, le droit des données à caractère personnel a été élaboré comme un régime préventif visant à anticiper et prévenir les risques d'atteinte à la personne[1055]. Pour des raisons historiques, liées à la centralisation des renseignements par les administrations (illustrée notamment par le projet SAFARI[1056]), le législateur français s'était surtout inquiété des menaces résultant de l'utilisation de l'informatique au sein de l'État[1057]. C'est ce qui explique que les règles issues de la loi du 6 janvier 1978 distinguaient les traitements opérés par le secteur public de ceux mis en œuvre par le secteur privé[1058]. Les traitements automatisés d'informations nominatives effectués par le secteur public n'étaient permis que suite à l'adoption d'un acte normatif pris après l'avis motivé de la CNIL[1059]. Les traitements effectués par le secteur privé bénéficiaient, quant à eux, d'un régime bien plus souple puisqu'ils devaient juste faire l'objet d'une déclaration préalable auprès de la CNIL[1060].

Ces règles déclaratives étaient complétées par des obligations relativement succinctes reprenant largement les principes du *code of fair information practices*. Ainsi, certaines dispositions avaient trait à la collecte et à la sécurité des données[1061], et des principes encadraient les transferts de données en dehors du territoire national[1062]. L'un des plus importants apports de la loi du 6 janvier 1978 a été de reconnaître certains droits aux personnes à l'égard de leurs informations, telles que la

---

[1055] Comme le remarquait Monsieur Pascal Ancel, la protection de la vie privée « passe surtout par la sanction des atteintes une fois qu'elles se sont produites. La loi de 1978 n'ignore pas ce point de vue : mais, parce qu'on a affaire à des atteintes difficiles à déceler, donc à sanctionner, elle organise aussi – et surtout – un système de prévention des atteintes éventuelles », P. Ancel, « La protection des données personnelles : aspects de droit privé français », *RID comp.* 1987, vol. 39, nº 3, p. 609, spéc. p. 614. À l'inverse, le régime de protection de la vie privée tend plutôt à réparer l'atteinte à la personne, en témoigne d'ailleurs sa construction jurisprudentielle initialement basée sur le fondement de la responsabilité civile extracontractuelle, V. *infra*, nº 321.
[1056] V. *supra,* nº 174.
[1057] Sur ce point, le rapport Tricot expliquait que « la conjonction des prérogatives de puissance publique et des moyens informatisés pose des problèmes qui, sous d'importantes réserves, ne se rencontrent pas au même degré dans le secteur privé. En outre, malgré la tendance au regroupement des entreprises, le secteur privé se caractérise encore par la coexistence et souvent la concurrence de nombreuses entités de volume moyen ou faible », v. B. Tricot, « Rapport de la commission Informatique et libertés », La Documentation française, 1975, p. 29.
[1058] G. Braibant, « Données personnelles et société de l'information. Rapport au Premier ministre sur la transposition en droit français de la directive nº 95/46 », La Documentation française, 1998, p. 37.
[1059] L'article 15 de la loi nº 78-17 du 6 janv. 1978 distinguait entre deux types d'actes normatifs : certains traitements devaient être autorisés par la loi, les autres étaient décidés par un acte réglementaire.
[1060] Art. 16, 17 et 19 de la loi nº 78-17 du 6 janv. 1978.
[1061] Art. 25 et 28 de la loi nº 78-17 du 6 janv. 1978.
[1062] Art. 24 de la loi nº 78-17 du 6 janv. 1978.

transparence sur les traitements, le droit d'accès aux données, le droit d'opposition aux traitements, et le droit à la rectification des données erronées[1063].

306. Un régime formaliste. L'image renvoyée par la loi du 6 janvier 1978 était celle d'un régime principalement administratif. La conformité aux lourdes obligations déclaratives et à quelques obligations de fond permettait de rendre licites les traitements d'informations nominatives. La loi ne prenait pas vraiment en considération les effets des traitements sur les personnes, sauf pour les traitements les plus intrusifs. En effet, seuls les traitements de données les plus sensibles[1064] et les décisions fondées sur un traitement automatisé d'informations nominatives[1065] étaient strictement encadrés. Ainsi, pour la grande majorité des traitements de données, leur finalité n'était pas considérée comme un élément déterminant de leur licéité. Pour le dire simplement, tant que le traitement respectait les règles administratives, celui-ci était considéré comme licite, même si ses conséquences étaient importantes sur la personne. C'est sans doute ce qui explique la place réduite attribuée à la réparation des atteintes résultant de ces traitements.

307. La place initialement limitée de la réparation des atteintes. En dépit de la volonté affichée de protéger les personnes contre les risques liés aux traitements informatiques, la loi du 6 janvier 1978 s'est relativement peu intéressée à la responsabilité des organismes. Seuls les traitements les plus intrusifs, c'est-à-dire ceux portant atteinte à la réputation, à la considération ou à l'intimité de la vie privée, étaient pénalement réprimés[1066]. Les autres sanctions instaurées par cette loi étaient liées aux manquements aux formalités préalables[1067]. Ainsi, les victimes de traitements illicites ne bénéficiaient pas de voies de recours spécifiques pour agir en réparation en cas de

[1063] En vertu de l'article 22 de la loi nº 78-17 du 6 janvier 1978, le droit d'accès était facilité par l'instauration d'une liste de traitements déclarés ou autorisés mise à disposition par la CNIL, v. *infra*, nº 310. Les autres droits étaient répartis au fil du texte, v. art. 3, 26, 27, 34, 35, 36, 39 et 40 de la loi nº 78-17 du 6 janv. 1978. Sur l'importance du droit à l'information pour la protection des personnes, v. N. Mallet-Poujol, « Protection des données personnelles et droit à l'information », *Légicom* 2017, nº 59, p. 49.

[1064] L'article 18 de la loi nº 78-17 du 6 janv. 1978 encadrait l'utilisation du répertoire national d'identification, l'article 30 restreignait le traitement des informations relatives aux infractions, condamnations ou mesures de sûreté, l'article 31 interdisait les traitements de données sensibles (données faisant apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales des personnes) et l'article 32 restreignait l'accès au fichier électoral.

[1065] L'article 2 de la loi nº 78-17 du 6 janvier 1978 interdisait la prise de décisions administratives, privées et de justice fondée sur un traitement automatisé.

[1066] Art. 43 de la loi nº 78-17 du 6 janv. 1978.

[1067] Art. 41 et 42 de la loi nº 78-17 du 6 janv. 1978. L'article 44 de la loi nº 78-17 du 6 janvier 1978 sanctionnait les traitements qui ne respectaient pas les finalités prévues par la déclaration ou autorisation.

manquement ou d'atteinte à leur personne[1068]. Sans doute, le législateur considérait que l'ancien article 1382 (désormais article 1240) du code civil pouvait servir de fondement pour de telles actions en responsabilité[1069]. Le régime mis en place en 1978 avait donc essentiellement un caractère administratif, et la personne concernée y avait une place limitée.

§ II. Le glissement vers un régime répressif

308. Plan. Le règlement européen a considérablement allégé les obligations déclaratives et a adopté un régime de responsabilité pour les organismes s'inspirant de certains principes à l'œuvre en droit américain (A). Le pendant d'un tel principe de responsabilité est le dispositif de sanctions dissuasives, transformant le droit des données personnelles en un droit répressif (B).

A. La consécration d'un principe de responsabilité fondé sur la confiance

309. Le passage d'un critère organique à un critère qualitatif. La transposition de la directive 95/46 a largement remanié le droit français des données personnelles[1070]. La distinction fondée sur le responsable du traitement est abandonnée au profit d'un critère fonctionnel lié au traitement effectué[1071]. Ainsi, à partir de 2004[1072], c'est la dangerosité du traitement qui déclenche le régime de formalités alourdies[1073]. Pour les traitements les plus courants considérés comme les moins dangereux, les obligations déclaratives sont amplement allégées. De nombreux traitements en sont complètement

---

[1068] Pour François Rigaux, ce droit d'action, reconnu aux individus et exercé devant les tribunaux de l'ordre judiciaire ou administratif, est symbolique, F. Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, Bruylant, 1990, nº 536, p. 596.

[1069] Pourtant, la preuve de la faute ou du préjudice est particulièrement difficile à apporter, v. *infra*, nºs 540 s. V. aussi, sur la difficulté d'apporter ces preuves en matière d'atteinte à la vie privée, P. Kayser, « Le secret de la vie privée et la jurisprudence civile », in *Mélanges R. Savatier*, Dalloz, 1965, p. 405 s., nº 7, spéc. p. 412.

[1070] Des signes de cette évolution étaient déjà visibles avant la transposition de la directive 95/46, v. not. J. Fauvet, « La protection des données personnelles », *RID comp.* 1987, vol. 39, nº 3, p. 551, spéc. p. 552. Ainsi, par exemple, dès janvier 2007, la Suède avait adopté un dispositif prévoyant des simplifications du régime pour les « traitements courants » et d'autres pays l'avaient rapidement rejointe, v. P. Blanc-Gonnet Jonason, « Vers une meilleure adaptation du droit de la protection des données personnelles à la réalité informationnelle », *AJDA* 2008, p. 2105 ; R. Gola, « Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », *Légicom* 2017, nº 59, p. 29.

[1071] La distinction opérée par la loi française entre les secteurs public et privé est abandonnée. Bien que de nature différente, les risques pour les personnes des traitements opérés par ces deux secteurs sont considérés tout aussi grands, v. G. Braibant, « Données personnelles et société de l'information. Rapport au Premier ministre sur la transposition en droit français de la directive nº 95/46 », La Documentation française, 1998, p. 37.

[1072] C'est la loi nº 2004-801 du 6 août 2004 qui a transposé, en droit français, la directive CE nº 95/46.

[1073] La loi de 2004 conserve une spécificité pour certains traitements issus du secteur public, notamment ceux liés aux traitements les plus dangereux, v. not. art. 25, 26, 27 et 29 de la loi nº 78-17 du 6 janv. 1978 telle que modifiée par la loi nº 2004-801 du 6 août 2004.

exonérés, et le nombre de déclarations simplifiées a largement augmenté[1074]. Cet allègement a été compensé par l'attribution à l'autorité de protection des données de pouvoirs de contrôle *a posteriori*[1075]. Ainsi, à partir de 2004, la CNIL a été dotée de pouvoirs de sanction[1076]. Après mise en demeure, l'institution peut prononcer à l'égard du responsable du traitement une sanction pécuniaire ou une injonction de cesser le traitement[1077].

310. Un régime critiqué. Malgré ces évolutions, le dispositif restait souvent critiqué. Il était considéré comme une charge administrative et financière inadaptée et inutile[1078]. Le règlement européen reconnaît d'ailleurs que les formalités prévues par la directive 95/46 n'ont pas « contribué à améliorer la protection des données à caractère personnel »[1079]. En pratique, ce régime était particulièrement lourd pour les organismes qui étaient tenus de respecter les formalités préalables dans chacun des États membres où ils opéraient, suivant des modalités variant d'un État à l'autre[1080]. Cette fragmentation territoriale a d'ailleurs été considérée comme une entrave au marché intérieur[1081].

Par ailleurs, l'obligation de déclaration préalable a eu tendance à créer une sorte de *momentum* pour les responsables du traitement. Effectuée en début de traitement, sans besoin d'être renouvelée, cette obligation présentait intrinsèquement un caractère

---

[1074] Par exemple, les traitements mis en œuvre par un responsable du traitement ayant désigné un Correspondant Informatique et Libertés étaient exemptés de ces formalités, v. A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, n^os^ 947 s., p. 379 s. Selon Madame Sophie Porteau-Azoulai, « l'idée inspirée (…) était qu'il fallait apporter un correctif au principe trop strict qui veut que la loi appréhende tous les traitements d'informations nominatives et non point seulement ceux susceptibles de porter atteinte à la vie privée et aux libertés », S. Porteau-Azoulai, *Le pouvoir réglementaire de la Commission nationale de l'informatique et des libertés,* th. Paris II, 1993, p. 60.

[1075] C. Bloud-Rey, « Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles », *D.* 2013, p. 2795, § 6.

[1076] Art. 17 de la loi n° 78-17 du 6 janv. 1978 telle que modifiée par la loi n° 2004-801 du 6 août 2004.

[1077] Art. 45 § I de la loi n° 78-17 du 6 janv. 1978 telle que modifiée par la loi n° 2004-801 du 6 août 2004. Avant cette modification, l'institution était plutôt chargée d'une mission de surveillance, pour laquelle il lui était notamment confié un pouvoir d'alerte. Par exemple, elle pouvait faire des dénonciations au procureur, v. *infra*, n° 521.

[1078] V. not. P. Blanc-Gonnet Jonason, « Vers une meilleure adaptation du droit de la protection des données personnelles à la réalité informationnelle », *AJDA* 2008, p. 2105.

[1079] Cons. 89 règlement UE n° 2016/679.

[1080] « Dans son évaluation du cadre juridique actuel, la Commission relevait que ces formalités se traduisent par un coût très élevé pour les entreprises, obligées de les respecter dans chacun des États membres où elles opèrent, suivant des modalités variant d'un État à l'autre », E. Brunet, « Règlement général sur la protection des données à caractère personnel – Genèse de la réforme et présentation globale », *Dalloz IP/IT* 2016, p. 567. V. aussi, N. Robinson, H. Graux, M. Botterman et L. Valeri, « Review of the European data protection directive », *Rand Europe* 2009, p. 31.

[1081] Le considérant 9 du règlement UE n° 2016/679 affirme d'ailleurs que « la fragmentation de la mise en œuvre de la protection des données dans l'Union » a pu « empêcher le libre flux de ces données dans l'ensemble de l'Union ».

ponctuel[1082]. Elle donnait la fausse impression que les traitements déclarés étaient conformes au droit Informatique et libertés[1083].

À ces critiques s'ajoutaient également les risques liés à la centralisation d'un tel fichier au sein d'une institution étatique, même lorsque celle-ci est déclarée « indépendante »[1084]. L'objectif initial de la loi Informatique et libertés était précisément de diminuer les capacités et pouvoirs de traitements des données effectués par l'État. Pourtant, en obligeant les responsables du traitement à les déclarer auprès d'une institution centrale, ce système instaurait ce contre quoi il était censé lutter[1085]. Cette critique devait toutefois être relativisée dès lors que la centralisation visait aussi à permettre aux personnes concernées d'avoir un point central concernant l'ensemble des traitements de données effectués sur le territoire national. En effet, l'article 22 de la loi du 6 janvier 1978 prévoyait la *mise à la disposition du public* de la liste des traitements déclarés afin d'encourager les personnes concernées à s'intéresser aux traitements effectués sur leurs données. En pratique, la CNIL n'a publié ce fichier qu'en 2017, atténuant ainsi fortement son utilité[1086].

Par ailleurs, l'obligation de déclaration, bien que peu contraignante, faisait l'objet de nombreux manquements par les organismes.

311. Les nombreux manquements aux obligations déclaratives. Plusieurs auteurs ont mis en évidence les carences déclaratives de multiples organismes[1087]. Face à ces manquements, la CNIL a été plutôt accommodante puisqu'elle a peu utilisé son pouvoir

---

[1082] Pour autant, l'obligation de déclaration était loin d'être la seule obligation prévue par ces règles, puisqu'elles s'accompagnaient notamment de certains principes de transparence et d'information et reconnaissaient aux personnes de nombreux droits sur leurs données.

[1083] Comme le remarquait Madame Anne Debet, « l'autorité administrative indépendante n'effectue, généralement, pas d'examen approfondi des 70 000 déclarations qui lui parviennent chaque année, et le contrôle est encore plus faible sur les déclarations simplifiées. Elle est, de plus, obligée de délivrer un récépissé sans délai, récépissé qui permet la mise en œuvre du traitement et donne donc vie à celui-ci, si le dossier est complet, sans pouvoir exercer de contrôle sur sa licéité », A. Debet, « Un fichier non déclaré à la CNIL est une chose hors du commerce », *JCP G* 2013, nº 37, p. 930. V. déjà, CE Sec., 6 janv. 1997, nº 159129, *Caisse d'épargne Rhône Alpes Lyon* c. *CNIL*, *Lebon* p. 7.

[1084] Sur l'indépendance de la CNIL, v. *infra*, nos 474 s.

[1085] Le rapport Tricot évoquait les risques liés à « la constitution de vastes "banques de données" et de réseaux d'ordinateurs susceptibles d'enregistrer, traiter et diffuser les informations les plus variées concernant les personnes, les entreprises et les groupements », B. Tricot, « Rapport de la commission Informatique et libertés », La Documentation française, 1975, p. 7.

[1086] CNIL, « Traitements de données personnelles déclarés à la CNIL avant le 25 mai 2018 », *data.gouv.fr* 11 oct. 2017. Jusqu'à cette date, il était possible d'en demander communication à l'institution en formulant une demande écrite.

[1087] P. Blanc-Gonnet Jonason, « Vers une meilleure adaptation du droit de la protection des données personnelles à la réalité informationnelle », *AJDA* 2008, p. 2105 ; D. Forest, « Trente ans et des poussières. Retour sur les premiers pas de la CNIL », *RLDI* 2008, nº 34, p. 77, spéc. p. 79.

de sanction[1088]. Pour justifier cette indulgence, l'institution a souvent invoqué une volonté d'aider les organismes à s'adapter à cette matière nouvelle et technique, ou encore l'insuffisance de ses moyens et pouvoirs juridiques[1089]. Ces justifications contrastent fortement avec l'interprétation très large de la notion de donnée à caractère personnel qu'elle retient depuis 1978, étendant *de facto* son domaine de compétence[1090].

Face à ce système critiqué et peu respecté, le législateur européen a acté son abandon au profit d'un régime de responsabilité.

312. L'abandon du système déclaratif. En dépit de réticences des négociateurs français[1091], le règlement européen a adopté un nouveau système de protection des données personnelles fondé sur le risque lié aux traitements[1092]. Le texte retient un principe de « responsabilisation » des organismes[1093] qui leur impose de documenter leur conformité. Ils doivent ainsi évaluer la nature, la portée, le contexte, les finalités et les risques du traitement afin de mettre en œuvre les mesures techniques et organisationnelles appropriées[1094]. Désormais, seuls les traitements les plus dangereux pour les libertés doivent faire l'objet d'une consultation préalable de l'autorité de contrôle. L'article 35 du règlement prévoit ainsi que, dans le cas où un traitement « est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes

[1088] « La CNIL qui a toujours estimé que c'était au responsable du traitement d'assumer sa responsabilité en appliquant la loi, qu'il ne lui revenait pas, faute de compétence et de moyens, d'engager la traque des traitements illégaux », A. Lucas, J. Devèze et J. Frayssinet, *Droit de l'informatique et de l'Internet*, PUF, 2001, nº 297, p. 170.
[1089] Comme le notait récemment Monsieur Michel Vivant, « En son temps, la CNIL avait même théorisé son non-usage en mettant en avant la fonction pédagogique qui, disait-elle, était la sienne », M. Vivant, « L'État de non-droit », *D.* 2019, p. 753. Pour Madame Christina Koumpli, la CNIL « s'est en réalité "auto-désinvestie" de ses missions préventives, perdant ainsi en légitimité », C. Koumpli, *Les données personnelles sensibles. Contribution à l'évolution du droit fondamental à la protection des données à caractère personnel*, th. Paris I, 2019, p. 496.
[1090] V. *supra,* nº 149.
[1091] E. Netter, *Numérique et grandes notions du droit privé. La personne, la propriété, le contrat*, mémoire en vue de l'habilitation à diriger des recherches en droit privé, Picardie, 20 nov. 2017, nº 68, p. 91.
[1092] E. Brunet, « Règlement général sur la protection des données à caractère personnel. Genèse de la réforme et présentation globale », *Dalloz IP/IT* 2016, p. 567.
[1093] Un tel principe n'est pas nouveau puisqu'il figurait déjà dans les lignes directrices de l'Organisation de coopération et de développement économiques (OCDE) régissant la protection de la vie privée adoptées en 1980 et modifiées en 2013, v. OCDE, Lignes directrices du 23 sept. 1980 sur la vie privée et les flux transfrontières de données à caractère personnel. L'OCDE a confirmé cette approche fondée sur la responsabilité dans le *Privacy framework* adopté en 2013. Le G29 avait également discuté de ce principe en 2010, G29, WP 173, Avis nº 3/2010 sur le principe de responsabilité, 13 juill. 2010.
[1094] Art. 5 et 24 § 1 du règlement UE nº 2016/679. Pour une brève présentation du principe de responsabilité applicable en droit des données à caractère personnel, v. N. Laneret, « L'*accountability* et la protection effective des données personnelles dans un monde digital connecté », *RUE* 2020, p. 35. Pour une analyse plus générale des codes de conduite et de leur valeur en tant que source du droit, v. M. Larouer, *Les codes de conduite, sources du droit*, th. Lyon, 2016, Dalloz.

physiques », le responsable du traitement est tenu d'effectuer une analyse d'impact[1095]. Lorsque celle-ci indique que le traitement présenterait un risque élevé s'il n'était pas mis en œuvre avec des mesures visant à atténuer ce risque, l'organisme doit consulter l'autorité de contrôle[1096]. Le règlement européen a donc amplement réduit les cas dans lesquels l'autorité de contrôle doit être informée des traitements de données mis en œuvre par les organismes.

313. La nouvelle notion en phase avec le régime de responsabilité. La notion de donnée à caractère personnel proposée s'inscrit dans la logique de responsabilité posée par le nouveau droit des données personnelles[1097]. Ce droit invite les organismes à mettre en œuvre toutes les mesures nécessaires au respect des principes relatifs aux traitements de données personnelles[1098]. Plusieurs mesures internes doivent donc être mises en place afin de garantir ce respect, sans que le règlement n'impose une approche de conformité uniforme. Le texte propose un ensemble d'instruments allant du registre des traitements[1099] à l'analyse d'impact sur la protection des données[1100] en passant par la nomination d'un délégué à la protection des données pilote de cette conformité[1101].

Dans tous les cas, la première étape de cette mise en conformité passe par un questionnement essentiel : l'organisme est-il en présence d'un traitement de données à caractère personnel ? Pour répondre à cette question, il doit s'interroger sur les données qu'il collecte et les traitements qu'il met en œuvre. Ainsi, la première étape liée à la qualification de la donnée invite l'organisme à étudier les finalités, les objectifs,

---

[1095] Sur les cas dans lesquels cette analyse est obligatoire, A. Debet et N. Métallinos, « Mise en conformité RGPD / Analyse d'impact. La CNIL publie la liste des traitements pour lesquels une analyse d'impact relative à la protection des données (AIPD) est requise », *CCE* 2019, nº 1, comm. 4.

[1096] Art. 36 du règlement UE nº 2016/679. À ces consultations s'ajoutent également l'ensemble des formalités préalables prévues par la loi française pour certains des traitements mis en œuvre dans le secteur public, v. not. art. 31 et 32 de la loi la loi nº 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018.

[1097] Pour une présentation du nouvel équilibre instauré par le règlement européen, v. not. R. Gola, « Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », *Légicom* 2017, nº 59, p. 29.

[1098] N. Laneret, « L'*accountability* et la protection effective des données personnelles dans un monde digital connecté », *RUE* 2020, p. 35.

[1099] Art. 30 du règlement UE nº 2016/679. Pour accompagner les responsables du traitement dans la mise en œuvre de leur registre, la CNIL a proposé un modèle de registre.

[1100] Art. 35 du règlement UE nº 2016/679. Afin d'aider les responsables du traitement dans cette analyse d'impact, la CNIL a développé le logiciel PIA pour faciliter la conduite et la formalisation des analyses d'impact relatives à la protection des données. Le G29 a également publié des lignes directrices sur le sujet, G29, WP 248 rév. 01, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est "susceptible d'engendrer un risque élevé" aux fins du règlement (UE) 2016/679, 4 oct. 2017.

[1101] Art. 37 s. du règlement UE nº 2016/679. Sur ces instruments, v. not. *JCl. comm.,* fasc. 942, « Le délégué à la protection des données (DPD) », par G. Desgens-Pasanau, 2018, nºs 36 s. ; O. Tambou, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, nºs 280 s., p. 249 s.

l'utilité et les effets de son traitement. La réponse à ces questionnements l'aide à déterminer la nature des données qu'il traite et lui permet ensuite d'appliquer le droit opportun : droit des données à caractère personnel ou libre circulation des données[1102]. Si l'organisme conclut que les données qu'il traite sont des données à caractère personnel, l'ensemble des analyses effectuées à ce stade pourront être conservées à des fins de documentation, notamment pour prouver sa conformité. La notion proposée s'articule donc très bien avec le régime mis en place par le règlement européen.

314. Le principe de responsabilité rapprochant le modèle européen du modèle américain. Le régime issu du règlement européen, souvent décrit comme un régime fondé sur l'*accountability*[1103], instaure une forme de « co-régulation entre les responsables de traitement et les autorités, consistant en la mise en place de programmes de conformité à l'intérieur des entreprises et la supervision de ces mesures par les autorités de l'État »[1104]. Ces formes de régulation sont connues de certaines branches du droit français, mais sont particulièrement développées aux États-Unis, et notamment dans le domaine des données personnelles[1105].

315. Les origines de la protection de la *privacy* aux États-Unis. Les premiers signes d'une protection civile de la *privacy*[1106] remontent à 1888 avec le *Traité sur la responsabilité civile* du juge Cooley[1107]. Celui-ci y définissait la *personal immunity*

[1102] Sur des traitements de données contenant plusieurs types de données, v. not. C. Zorn, « Le jeu de données composites : données personnelles et (en même temps) non personnelles ? », *Dalloz IP/IT* 2020, p. 420.
[1103] Selon l'Organisation internationale de normalisation (ISO), l'*accountability* est une obligation de diligence à laquelle s'ajoute l'adoption de mesures concrètes et pratiques assurant la protection des données, v. ISO/IEC, « 29100 : Information Technology – Security techniques – Privacy framework », 2011.
[1104] W. Maxwell et S. Taïeb, « L'*accountability,* symbole d'une influence américaine sur le règlement européen des données personnelles ? », *Dalloz IP/IT* 2016, p. 123. Pour une analyse de cette forme de régulation, v. M.-A. Frison-Roche, « Le droit de la *compliance* », *D.* 2016, p. 1871 ; M.-A. Frison-Roche, « Le droit de la *compliance* au-delà du droit de la régulation », *D.* 2018, p. 1561 ; M.-E. Boursier, « Qu'est-ce que la *compliance* ? Essai de définition », *D.* 2020, p. 1419. Pour une étude de la *compliance* en matière de données à caractère personnel, K. Favro, « La démarche de *compliance* ou la mise en œuvre d'une approche inversée », *Légicom* 2017, nº 59, p. 21.
[1105] J. Frayssinet, « La protection des données personnelles est-elle assurée sur l'Internet ? », in *Le droit international de l'Internet,* Bruylant, dir. G. Chatillon, 2003, p. 438. Pour une analyse des convergences entre le modèle européen et le modèle américain sur le principe d'*accountability,* S. Puillaude, « La protection des données à caractère personnel : importation du modèle américain au sein de l'Union européenne », mémoire de Master 2 Paris II, 2016.
[1106] Comme le remarquait François Rigaux en 1980, « les termes *privacy* et *right of privacy* sont d'une traduction malaisée, comme en témoignent les hésitations des rédacteurs des instruments internationaux ». Parfois l'expression « privacy » renvoie à la vie privée, d'autres fois, dans certains contextes, les mots *intimité, anonymat* ou *secret* expriment plus correctement cette expression, F. Rigaux, « L'élaboration d'un "right to privacy" par la jurisprudence américaine », *RID comp.* 1980, vol. 32, nº 4, p. 701. L'usage du terme anglais sera privilégié dans la suite de notre étude.
[1107] T. Cooley, *A treatise on the law of torts or the wrongs which arise independent of contract*, vol. 1, 2e éd., Callaghan and Company, 1888, p. 29.

comme le droit « d'être laissé tranquille » (*the right to be let alone*). Deux ans plus tard, Samuel Warren et Louis Brandeis publiaient *The right to privacy* dans la prestigieuse revue juridique de Harvard[1108]. Cet article, d'une clarté académique sans pareille, appelait à l'émergence d'une protection juridique de la *privacy*[1109]. Pour renforcer leurs propos, ses auteurs dénonçaient les pratiques de la presse écrite et énonçaient les risques que ces abus peuvent engendrer pour les personnes et leur libre développement[1110]. Ils concluaient leur article en revendiquant l'existence d'un droit à la *privacy,* d'un droit « d'être laissé tranquille »[1111]. Bien que cet article ait été qualifié comme « le plus influent article de doctrine jamais écrit »[1112], son écho législatif et jurisprudentiel a finalement été assez limité[1113]. En effet, il a fallu attendre 1960 pour que le droit civil à la *privacy* prenne un véritable essor aux États-Unis, notamment grâce à William Prosser. Après avoir étudié méthodiquement les quelques 300 affaires jugées entre 1890 et 1960 impliquant le droit au respect de la *privacy*, William Prosser a systématisé ce droit[1114]. Il avait décomposé la protection de la *privacy* en quatre délits civils : l'intrusion dans la vie personnelle d'un individu[1115] ; la divulgation publique de faits personnels[1116] ; le fait de rendre public des informations présentant une personne sous un mauvais jour[1117] et l'appropriation du nom ou de l'image d'une personne[1118]. L'influence de cet article est indéniable[1119], et il est clair qu'il a largement contribué à l'harmonisation de la jurisprudence dans les différents États en matière d'atteinte à la

---

[1108] L. Brandeis et S. Warren, « The right to privacy », *Harvard Law Review* 1890, vol. 4, p. 193 s. [4 HARV. L. REV. 193]. Plus tôt cette même année, un autre article relatif à la question de la protection des droits individuels avait été publié, E. Godkin, « The right to a citizen – to his reputation », *Scribner's Magazine* July 1890, p. 58.
[1109] L. Brandeis et S. Warren, « The right to privacy », *Harvard Law Review* 1890, vol. 4, p. 193 s. [4 HARV. L. REV. 193], spéc. p. 195 s.
[1110] Pour une étude plus détaillée des nouvelles formes d'atteintes aux personnes permises par les traitements, v. *infra*, n^os^ 387 s.
[1111] W. Wienczyslaw, « Le "droit à l'intimité" aux États-Unis », *RID comp.* 1965, vol. 17, n° 2, p. 365 s., spéc. p. 366.
[1112] H. Kalven, « Privacy in tort law – were Warren and Brandeis wrong ? », *Law & Contemporary Problems* 1966, vol. 31, p. 326 s. [39 LAW & CONTEMP. PROBS. 326], spéc. p. 327.
[1113] Les juridictions rendaient des décisions divergentes sur ce thème. Sur les refus de reconnaître le droit à la *privacy* comme un délit civil, v. not. Cour suprême de l'État de Rhode Island, 22 juin 1909, *Henry* c. *Cherry & Webb*, 30 R. I. 13 ; Cour suprême de l'État de Washington, 6 sept. 1911, *Hillman* c. *Star Pub. Co.*, 64 Wash. 691. Au contraire, sur la reconnaissance de ce droit, v. not. Cour fédérale d'appel du Kentucky, 19 juin 1909, *Foster-Milburn Co* c. *Chinn*, 134 Ky. 424 ; Cour fédérale d'appel du Missouri, 30 janv. 1911, *Munden* v. *Harris*, 153 Mo. App. 652. Ce n'est qu'en 1965 que la Cour suprême affirme la protection de la *privacy* sur le fondement de la responsabilité civile, v. Cour suprême des États-Unis d'Amérique, 7 juin 1965, *Griswold* c. *State of Connecticut*, 381 U.S. 479.
[1114] W. Prosser, « Privacy », *California Law Review* 1960, vol. 48, p. 383 s. [48 CAL. L. REV. 383].
[1115] W. Prosser, « Privacy », *California Law Review* 1960, vol. 48, p. 383 s. [48 CAL. L. REV. 383], spéc. p. 389 s.
[1116] W. Prosser, « Privacy », *California Law Review* 1960, vol. 48, p. 383 s. [48 CAL. L. REV. 383], spéc. p. 392 s.
[1117] W. Prosser, « Privacy », *California Law Review* 1960, vol. 48, p. 383 s. [48 CAL. L. REV. 383], spéc. p. 398 s.
[1118] W. Prosser, « Privacy », *California Law Review* 1960, vol. 48, p. 383 s. [48 CAL. L. REV. 383], spéc. p. 401 s.
[1119] N. Richards et D. Solove, « Prosser's privacy law : a mixed legacy », *California Law Review* 2010, vol. 98, p. 1887 s. [98 CAL. L. REV. 1887], spéc. p. 1888.

privacy[1120]. Certains États ont même repris cette structure directement dans leur droit écrit. Toutefois, ces délits n'ont pas réussi à s'adapter aux évolutions technologiques[1121]. En effet, l'un des critères pour caractériser la plupart de ces délits civils est que l'atteinte à la *privacy* doit être « hautement préjudiciable pour une personne raisonnable »[1122]. Dans l'environnement numérique, une telle preuve est très difficile à apporter puisque la collecte de données se fait souvent *via* une pluralité de données qui revêtent rarement ces caractéristiques[1123]. Plutôt que d'assouplir ces critères et de les adapter aux besoins sociaux et technologiques, les tribunaux se sont souvent contentés de vérifier qu'ils étaient réunis. La conséquence de cette interprétation stricte est que ces délits sont peu invoqués par les plaignants[1124].

Par ailleurs, deux limites ont entravé le développement d'une protection renforcée de la *privacy* aux États-Unis. La première est liée à la *third party doctrine* qui tient pour non protégées les données personnelles remises à un tiers, de sorte que les protections prévues par le Quatrième amendement ne leur sont pas applicables[1125]. La seconde est liée à la place centrale occupée par la liberté d'expression dans le système américain.

316. La place centrale de la liberté d'expression aux États-Unis. L'une des principales caractéristiques du droit américain est la protection accordée à la liberté d'expression. Le Premier amendement impose un principe de liberté de circulation de l'information comme prérequis à la liberté d'expression, laquelle est une pierre angulaire de ce système démocratique[1126]. Ainsi, par principe, la collecte et l'utilisation

---

[1120] T. McCarthy, « Prosser's four torts of privacy. Impact of Prosser's four torts and the 1977 Second Restatement of Torts », in *The Rights of Publicity and Privacy*, dir. T. McCarthy et R. Schechter, 2e éd., Thomson Reuters, 2020, no 1:24.

[1121] N. Richards et D. Solove, « Prosser's privacy law : a mixed legacy », *California Law Review* 2010, vol. 98, p. 1887 s. [98 CAL. L. REV. 1887], spéc. p. 1917.

[1122] Restatement (Second) of Torts, § 652, (1977).

[1123] V. not. cour d'appel d'Ohio, 19 juin 1975, *Shibley* c. *Time Inc.,* 45 Ohio App. 2d 69 ; cour d'appel d'Illinois, 30 juin 1995, *Dwyer* c. *American Express Co.*, 273 Ill. App. 3d 742.

[1124] R. Connallon, « An integrative alternative for America's privacy torts », *Golden Gate University Law Review* 2007, vol. 38, p. 71 s. [38 GOLDEN GATE U. L. REV. 71], spéc. p. 88.

[1125] Plus spécifiquement, les données personnelles volontairement remises à des tiers tels que les banques, les compagnies de téléphonie, les fournisseurs d'accès à Internet, n'entrent pas dans le domaine du Quatrième amendement. Il en résulte qu'en principe, la police peut accéder à ces données (v. Cour suprême des États-Unis d'Amérique, 21 avril 1976, *United States* c. *Miller,* 425 U.S. 435 et Cour suprême des États-Unis d'Amérique, 20 juin 1979, *Smith* c. *Maryland,* 442 U.S. 735). Pour autant, depuis quelques années, cette doctrine trouve des tempéraments. En 2014 par exemple, avec l'arrêt *Riley* c. *California*, la Cour suprême a étendu la protection de cet amendement aux utilisateurs de *smartphones* (Cour suprême des États-Unis d'Amérique, 25 juin 2014, *Riley* c. *California,* 573 U.S. 373). En 2018, l'arrêt *Carpenter* la Cour suprême a considéré que la police ne peut, sans mandat d'un juge, localiser les utilisateurs de *smartphone* qu'elle doit surveiller (Cour suprême des États-Unis d'Amérique, 22 juin 2017, *Carpenter* c. *United States,* 585 U.S.). Pour une brève analyse de ces évolutions, É. Zoller, « Cour suprême des États-Unis : Session d'octobre 2017 », *RDP* 2018, no 6, p. 1761.

[1126] E. Chemerinsky, *Constitutional law: principles and policies*, 6e éd., Wolters Kluwer, 2019, § 11.1 s., p. 1002 s.

des données, même personnelles ou sensibles, sont permises[1127]. Les restrictions à ce principe sont strictement encadrées[1128]. C'est l'une des raisons qui explique la place relative de la protection de la *privacy* dans le système américain.

317. Le développement de la *information privacy.* Dans les années 1960 et 1970, les traitements informatiques se sont considérablement développés, notamment dans le secteur privé[1129]. Ces développements ont attiré l'attention de la doctrine et du grand public. L'un des premiers domaines du secteur privé à s'informatiser et à collecter massivement des données sur les individus a été le secteur de l'évaluation du crédit. Ce secteur repose sur l'attribution par des agences d'évaluation du crédit d'une note censée refléter la capacité d'une personne à rembourser ses dettes[1130]. Cette note était établie à partir de nombreuses informations personnelles obtenues par des moyens variés. Par exemple, il était possible d'aller demander aux voisins d'une personne ce qu'ils pensaient d'elle et d'ajouter ensuite cette information à son dossier. C'est ce qui explique la présence de nombreuses erreurs dans ces fichiers. Ces erreurs avaient d'importantes conséquences sur la vie des consommateurs, puisque cette note influençait les taux d'emprunt ou les embauches. Pendant longtemps, les agences d'évaluation du crédit refusaient d'accorder aux personnes concernées un droit d'accès à leurs informations[1131]. Face aux critiques de plus en plus importantes contre ce système, le sénateur William Proxmire avait préparé une proposition de loi ambitieuse[1132]. Pour éviter l'adoption de ces dispositions jugées trop contraignantes, d'autres sénateurs avaient ajouté, au sein d'une proposition de loi en cours d'examen,

---

[1127] P. Schwartz et K.-N. Peifer, « Transatlantic data privacy law », *Georgetown Law Journal* 2017, vol. 106, p. 115 s. [106 GEO. L.J. 115], spéc. p. 136.

[1128] Seuls certains cas permettent de justifier des restrictions à la liberté d'expression : soit la loi est validée après un contrôle judiciaire très strict (v. par ex., Cour suprême des États-Unis d'Amérique, 23 juin 2011, *Sorrell* c. *IMS Health Inc.,* 564 U.S. 552, spéc. p. 579) ; soit la restriction entre dans une des catégories d'exception reconnues ; soit elle n'a qu'un effet négligeable sur le Premier amendement, v. J. Humbach, « Privacy and the right to free expression », *First Amendment Law Review* 2012, vol. 11, p. 16 s. [11 FIRST AMEND. L. REV. 16], spéc. p. 16.

[1129] Bien sûr, c'était initialement surtout le secteur public qui avait recours à l'informatique. Par exemple, la *National Security Agency* avait un rôle de centralisation des données de renseignement dès les années 1940, T. Burns, « The origins of the National Security Agency 1940 – 1952 », *NSA* 1990.

[1130] P. Swire, « Financial privacy and the theory of high-tech government surveillance », *Washington University Law Quarterly* 1999, vol. 77, p. 461 s. [77 WASH. U. L.Q. 461], spéc. p. 465.

[1131] S. Garfinkel, *Database Nation, The Death of Privacy in the 21st Century*, O'Reilly, 2000, p. 22 ; A. Miller, *Assault on Privacy, Computers, Data Banks, and Dossiers*, The University of Michigan Press, 1971, p. 69 s. La doctrine n'a pas manqué de critiquer ce refus, notamment parce que l'accès à ces données était permis pour toutes les autres personnes qui le demandaient.

[1132] E. Hendricks, *Credit scores & credit reports, how the system really works, what you can do*, 3e éd., Privacy Times, 2007, p. 180.

des articles sur ce sujet[1133]. Adoptée en 1970, la loi relative à l'évaluation équitable du crédit (*Fair Credit Reporting Act*[1134]) fut la première loi fédérale à protéger les données personnelles (*information privacy*)[1135]. Elle a ouvert la voie à de nombreuses autres règles fédérales dans les années suivantes. Par exemple, le *Privacy Act* de 1974[1136] qui protège les informations contenues dans les dossiers de l'administration, le *Family Educational Rights and Privacy Act* (FERPA) de 1974[1137] qui protège les dossiers scolaires, le *Cable Communications Policy Act* de 1984[1138] qui accorde des protections aux données détenues par les câblo-opérateurs et prestataires de services, le fameux *Health Insurance Portability and Accountability Act* (HIPAA) de 1996[1139] qui protège les données de santé, le *Telecommunications Act* de 1996[1140] qui prévoit des protections dans le domaine des télécommunications, le *Children Online Privacy Protection Act* (COPPA) de 1998[1141] qui protège les données des mineurs, et le *Gramm-Leach Bliley Act* (GLBA) de 1999[1142] qui règlemente le traitement d'informations personnelles non publiques dans le secteur bancaire. Cet ensemble disparate de lois sectorielles a instauré

[1133] Cette anecdote reflète relativement bien la dynamique législative à l'œuvre dans le domaine de la *privacy*. Lorsque des sénateurs favorables à des dispositions ambitieuses réussissent à obtenir un seuil d'adhésion suffisant, ils sont contrés par d'autres sénateurs qui réussissent à imposer une vision moins protectrice de la *privacy*.

[1134] Fair Credit Reporting Act, adopté le 26 octobre 1970 et entré en vigueur le 25 avril 1971, codifié dans le titre 15 du *United States Code Annoted*, aux sections 1681 et suivantes (15 U.S.C. § 1681).

[1135] E. Hendricks, *Credit scores & credit reports, how the system really works, what you can do*, 3e éd., Privacy Times, 2007, p. 12.

[1136] 5 U.S.C. § 552 (2000). Pour une étude sur la jurisprudence et la loi, v. Department of Justice, *Overview of the Privacy Act of 1974*, 2015. V. également, N. Richards, « Reconciling data privacy and the First amendment », *UCLA Law Review* 2005, vol. 52, p. 1149 s. [52 UCLA L. REV. 1149], spéc. p. 1167.

[1137] Pub. L. du 21 août 1974, nº 93-380, codifiée au 20 U.S.C. § 1221 et § 1232 s. Le *Family Educational Rights and Privacy Act* (FERPA) protège les données des élèves d'un accès ou d'une diffusion non autorisés.

[1138] Pub. L. du 30 oct. 1984, nº 98-549, codifiée au 47 U.S.C. § 521 s. Cette loi garantit la protection des données personnelles des consommateurs en ce qui concerne la collecte, la diffusion, la conservation et la destruction de ces données par des fournisseurs de télévision par câble.

[1139] Pub. L. du 21 août 1996, nº 104-191, codifiée au 42 U.S.C. § 1320 s. En 1996, la loi reportait l'adoption de règles spécifiques sur la protection des données médicales. Ce n'est qu'en 2003 et 2005 que ces règles ont été adoptées, v. *Privacy Rule* du 14 août 2002 Fed. Reg., vol. 67, nº 157, p. 53182 et *Security Rule* du 20 févr. 2003, Fed. Reg., vol. 68, nº 34, 20 févr. 2003, p. 8334. Ces règles ont été significativement réformées par le *Health Information Technology for Economic and Clinical Health Act* de 2009, (HITECH Act), Pub. L. du 17 févr. 2009, nº 111-5, qui élargit le champ d'application de HIPAA, renforce les sanctions en cas de violation et prévoit une obligation de notification en cas de violation de données couvertes par ces règles.

[1140] Pub. L. du 3 janv. 1996, nº 104-104, codifiée au 47 U.S.C. § 151 s. Cette loi vise à protéger l'accès, l'utilisation et la diffusion des informations liées à un utilisateur de réseaux de télécommunications.

[1141] Pub. L. du 21 avr. 2000, nº 105-277, codifiée au 15 U.S.C. § 6501 s. Le *Children's Online Privacy Protection Act* (COPPA) protège les données à caractère personnel d'enfants âgés de moins de 13 ans collectées en ligne.

[1142] Pub. L. du 12 nov. 1999, nº 106-102, codifiée au 15 U.S.C. § 6801 s. Les dispositions relatives à la *privacy* ont été ajoutées dans cette loi grâce au soutien du sénateur Joe Barton. Sa banque avait vendu ses informations personnelles à l'entreprise de lingerie *Victoria's Secret* qui lui adressait régulièrement des publicités. Ces envois dérangeaient le sénateur qui ne voulait pas que sa femme pense qu'il achetait de la lingerie pour une autre femme ou qu'il regardait ces catalogues. Sur cette anecdote, v. C. Hoofnagle et E. Honig, « Victoria's Secret and Financial Privacy », *EPIC* 2005. Cette loi pose le principe selon lequel les institutions financières concernées par le GLBA doivent assurer la sécurité des données personnelles qu'elles conservent et ne doivent pas divulguer les renseignements personnels non publics qu'elles détiennent à des tiers non affiliés, v. not. P. Swire, « The surprising virtues of the new financial privacy law », *Minnesota Law Review* 2002, vol. 86, p. 1263 s. [86 MINN. L. REV. 1263] ; R. Link, « Validity, Construction, and Application of Information Privacy Provisions of Gramm-Leach-Bliley Act », *American Law Reports* 2005, vol. 5, p. 497 s. [5 A.L.R. FED. 2d 497].

un régime de protection de la *information privacy* fragmenté, complexe et peu cohérent. La plupart du temps, les lois contenant des dispositions relatives à la *privacy* visent plutôt à réguler un secteur d'activité qu'à accorder une protection aux personnes. Ces dispositions spécifiques se fondent sur les principes issus du *code of fair information practices*[1143] et sont construites de manière similaire : elles protègent les données visées par la loi, ne s'appliquent qu'aux acteurs spécifiquement identifiés et accordent certains droits aux individus[1144]. Ces lois illustrent très bien la vision américaine selon laquelle le droit ne peut répondre, à lui seul, à l'ensemble des atteintes à la personne que la technique engendre. Ce système reconnaît donc une place importante à l'autorégulation[1145].

318. L'importante place de l'autorégulation dans le droit américain. En l'absence de fortes contraintes légales, et pour conserver la confiance des utilisateurs dans les services numériques, les entreprises et les régulateurs américains ont privilégié la voie de l'autorégulation[1146]. Certains organismes ont mis en œuvre des bonnes pratiques et créé des codes de conduite[1147]. Ce système a également favorisé le développement de technologies renforçant la protection de la vie privée[1148]. Pour autant, ce régime a montré ses limites et fait l'objet d'importantes critiques.

319. Critique du modèle américain. Beaucoup de critiques ont résonné contre le système américain en considérant qu'il n'était pas efficace pour protéger efficacement la *privacy*[1149]. L'une des critiques récurrentes est le niveau relativement faible de la protection des personnes, ainsi que le champ d'application réduit des lois qui ne permet

---

[1143] M. Rotenberg, « Fair information Practices and the Architecture of Privacy (What Larry Doesn't Get) », *Stanford Technology Law Review* 2001, p. 1 s. [2001 STAN. TECH. L. REV. 1], spéc. p. 36.
[1144] L'application restrictive des règles HIPAA permet notamment aux entreprises comme Google ou Facebook de traiter des données de santé pour leur propre compte sans avoir à respecter ces principes.
[1145] M. Cope Huie, S. Laribee et S. Hogan, « The right to privacy in personal data : the EU prods the U.S. and controversy continues », *Tulsa Journal of Comparative and International Law* 2002, vol. 9, p. 391 s. [9 TULSA J. COMP. & INT'L L. 391], spéc. p. 406.
[1146] S. Listokin, « Industry self-regulation of consumer data privacy and security », *The John Marshall Journal of Information Technology & Privacy Law* 2015, vol. 32, p. 15 s. [32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 15].
[1147] C. Hoang, « In the middle : creating a middle road between U.S. and EU data protection policies », *National Administrative Law Judge Foundation* 2012, vol. 32, p. 810 s. [32 J. NAT'L ASS'N L. JUDICIARY 810], spéc. p. 814 s.
[1148] V par ex. le déploiement d'outils de confidentialité tels que la *Platform for Privacy Preferences* (P3P). Ce projet, à l'initiative du consortium *World Wide Web Consortium* (W3C), a été approuvé en avril 2002. Il vise à standardiser le moyen par lequel un site web peut informer l'internaute de sa politique en matière de protection des données. Plus récemment, les projets autour de la protection de la *privacy* menés par le *National Institute of Standard and Technology* (NIST) témoignent de l'importance de la technologie dans la protection de la *privacy*, NIST, Privacy Framework, janv. 2020 ; NIST, Privacy Engineering Program, août 2017.
[1149] V. not. B. Fairclough, « Privacy piracy : the shortcomings of the United States' data privacy regime and how to fix it », *Journal of Corporation Law* 2016, vol. 42, p. 461 s. [42 J. CORP. L. 461], spéc. p. 466 s.

pas de s'adapter aux évolutions technologiques. Certains auteurs considèrent également que la participation de l'industrie à l'élaboration des standards et codes de conduite a nécessairement pour effet d'entraîner des conflits d'intérêts puisque les organismes peuvent avoir des intérêts contradictoires[1150]. Par exemple, monnayer les données personnelles ne semble pas compatible avec le principe de confidentialité des données.

L'absence d'institution chargée de veiller, de manière transversale et cohérente, au respect de la protection de la *privacy* s'ajoute aux critiques formulées à l'égard du modèle américain[1151]. Aux États-Unis, chaque loi désigne une commission ou un comité pour assurer, de manière plus ou moins directe, la protection de la *privacy*. En dépit de cette diversité, la *Federal Trade Commission* (FTC), commission chargée d'appliquer le droit de la consommation et d'assurer le respect des règles liées à la concurrence, occupe une place importante dans le domaine de la *privacy*[1152]. Par exemple, elle a réaffirmé certains grands principes, comme les *Fair Information Practices*[1153], et dans les années 2000, elle a largement œuvré pour que les sites Internet adoptent des politiques de confidentialité[1154]. La FTC a encouragé cette pratique, alors même que les politiques de confidentialité sont reconnues comme des instruments inefficaces pour protéger la vie privée des personnes[1155]. Toutefois, les manquements aux engagements pris dans les politiques de confidentialité lui permettent ensuite d'engager la responsabilité des entreprises. La FTC aurait ainsi engagé environ 215 actions de ce type[1156]. Le plus souvent, ces actions se clôturent par un accord amiable entre la FTC et l'entreprise concernée[1157].

Deux sanctions, l'une contre Google d'un montant de 22,5 millions de dollars et l'autre contre Facebook d'un montant de 5 milliards de dollars, ont toutefois été

[1150] V. not. R. Moshel, « … and then there was one : the outlook for a self-regulatory United States amidst a global trend toward comprehensive data protection », *Texas Tech Law Review* 2005, vol. 37, p. 357 s. [37 TEX. TECH. L. REV. 357], spéc. p. 367.

[1151] Les *State Attorneys General* (procureurs généraux de l'État) occupent une place de plus en plus importante dans la mise en œuvre de la protection des données personnelles. Pour une analyse très complète, v. D. Citron, « The privacy policymaking of State Attorneys General », *Notre Dame Law Review* 2017, vol. 92, p. 747 s. [92 NOTRE DAME L. REV. 461].

[1152] C. Hoofnagle, *Federal Trade Commission. Privacy law and policy*, Cambridge University Press, 2016.

[1153] FTC, « Privacy Online : Fair Information Practices in the Electronic Marketplace, A Report to Congress », mai 2000.

[1154] S. Hetcher, « The FTC as Internet privacy norm entrepreneur», *Vanderbilt Law Review* 2000, vol.53, p. 2041 s. [53 VAND. L. REV. 2041], spéc. p. 2044 et p. 2047.

[1155] A. McDonald et L. Faith Cranor, « The cost of reading privacy policies », *I/S: A Journal of Law and Policy for the Information Society* 2008-2009, vol. 4, p. 543 s. [4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 543] ; D. Cohen, « Le juge européen et les données personnelles », in *Mélanges R. Badinter*, Dalloz, 2016, p. 249 s., spéc. p. 253 ; N. Robinson, H. Graux, M. Botterman et L. Valeri, « Review of the European data protection directive », *Rand Europe* 2009, p. 29.

[1156] V. le site de la FTC, notamment la page liée à ses actions de « *enforcement* ».

[1157] D. Solove et W. Hartzog, « The FTC and the new common law of privacy », *Columbia Law Review* 2014, vol. 114, p. 583 s. [114 COLUM. L. REV. 583], spéc. p. 610 s.

prononcées pour non-respect des engagements pris à l'égard de la FTC[1158]. Ces sanctions, loin d'être égalées en Europe[1159], montrent qu'en dépit d'un droit moins contraignant, les autorités tentent de faire respecter des principes de protection et les engagements des entreprises. En plus d'imposer des sanctions importantes, ces accords amiables obligent les organismes à mettre en œuvre des changements structurels au sein de leur organisme. Par exemple, en plus de la sanction de 5 milliards de dollars, l'accord amiable entre la FTC et Facebook impose à l'entreprise et ses filiales des modifications importantes dans leurs pratiques relatives à la *privacy,* en imposant notamment un système de surveillance plus strict des développeurs tiers, une interdiction d'utiliser pour d'autres finalités les numéros de téléphone obtenus pour des raisons de sécurité, un encadrement de la reconnaissance faciale ou la mise en œuvre d'un programme de sécurité transversal[1160].

En laissant une plus grande souplesse dans la mise en œuvre de ses règles, le législateur européen a rapproché le droit européen de la protection des données personnelles du droit américain[1161]. Toutefois, la mise en œuvre de ce principe en Europe est beaucoup plus encadrée qu'aux États-Unis puisqu'elle est assortie de contraintes et d'obligations[1162].

B. L'élaboration d'un dispositif de sanctions dissuasives

320. Le pendant du principe de responsabilité en Europe : les sanctions. Un proverbe russe affirme « Доверяй, но проверяй », pouvant être traduit littéralement

---

[1158] Sur l'affaire Google, v. FTC, « Google will pay $22.5 million to settle FTC charges it misrepresented privacy assurances to users of Apple's Safari Internet browser », 9 août 2012 ; v. not. S. Vergnolle, « Google passe à la caisse… Des cookies à 22,5 millions de dollars ! », *Blog MBDE* 2013. Sur l'affaire Facebook, v. FTC, « FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook », 24 juill. 2019 ; v. not. W. Maxwell, « Amende contre Facebook : comment la FTC américaine s'est transformée en "super CNIL" », *The Conversation* 11 août 2019.

[1159] La plus importante sanction européenne a été imposée à l'égard de Google par la CNIL française et s'est élevée à 50 millions d'euros, CNIL, délibération nº 2019-001 du 21 janvier 2019 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google LLC. Cette délibération a été confirmée par le Conseil d'État, CE Sec., 19 juin 2020, *Société Google LLC*, nº 430810, *Lebon*.

[1160] FTC, « Complaint for civil penalties, injunction, and other relief », 24 juin 2019. Pour une brève presentation de l'accord, v. L. Fair, « FTC's $5 billion Facebook settlement : record-breaking and history-making », *ftc.gov* 24 juin 2019.

[1161] Pour une analyse des différences entre l'autorégulation et la co-régulation, v. D. Hirsch, « The law and policy of online privacy : regulation, self-regulation, or co-regulation ? », *Seattle University Law Review* 2011, vol. 34, p. 439 s. [34 SEATTLE U. L. REV. 439], spéc. p. 451 s.

[1162] Sur les liens entre les deux systèmes, v. not. C. Castets-Renard, « Quels liens établir entre les USA et l'UE en matière de vie privée et protection des données personnelles ? », *Dalloz IP/IT* 2016, p. 115 ; P. Schwartz et K.-N. Peifer, « Transatlantic data privacy », *Georgetown Law Journal* 2017, vol. 106, p. 115 s. [106 GEORGETOWN L.J. 115]. V. aussi, J. Whitman, « The two western cultures of Privacy : dignity versus liberty », *The Yale Law Journal* 2004, vol. 113, p. 1151 s. [113 YALE L.J. 1151]. Comp. J.-L. Halpérin, « Protection de la vie privée et privacy : deux traditions juridiques différentes ? », *Les Nouveaux Cahiers du Conseil constitutionnel* 2015, nº 48, p. 59.

par « Faites confiance, mais vérifiez »[1163]. Ce proverbe se transpose particulièrement bien au nouveau droit des données à caractère personnel. Celui-ci pose un principe de confiance mais appelle à une augmentation des contrôles et la possibilité d'imposer des sanctions importantes en cas de manquement.

Classiquement, la sanction est présentée comme le moyen le plus sûr d'assurer le respect de la règle de droit, puisque sa fonction première serait de garantir l'effectivité de la règle juridique, sa réalisation dans les faits[1164]. La majorité des auteurs s'accordent sur le fait que le pouvoir de prononcer d'importantes sanctions constitue le gage de l'effectivité du dispositif mis en place par le règlement européen[1165]. Les sanctions auraient ainsi un rôle dissuasif[1166]. Pour Monsieur Emmanuel Netter, le principe de responsabilité du droit des données personnelles serait difficilement défendable s'il n'était pas adossé à des sanctions très élevées, susceptibles d'être infligées à celui qui aurait trahi la confiance accordée[1167]. À cet égard, le dispositif de sanctions instauré est particulièrement étendu et l'autorité de contrôle y occupe une place essentielle[1168]. L'article 45 du règlement européen établit une longue liste des sanctions susceptibles d'être prononcées par les autorités de contrôle : ces sanctions vont d'un simple rappel à l'ordre au prononcé d'une interdiction de traiter des données, en passant par d'importantes amendes administratives[1169]. C'est surtout l'augmentation considérable du montant des sanctions qui a placé le droit des données à caractère personnel comme l'une des priorités des entreprises. En cas de manquement, elles risquent d'être condamnées à payer des amendes pouvant atteindre 10 à 20 millions d'euros ou des amendes calculées à partir de leur chiffre d'affaires annuel mondial (une part entre 2 à 4 %), le montant le plus

---

[1163] Ce proverbe était l'une des phrases fétiches du Président américain Ronald Reagan. Il l'a notamment employé lors de la signature du traité sur les forces nucléaires à portée intermédiaire, Opinion, « Trust, but verify », *The New York Times* 10 déc. 1987.

[1164] Sur cette vision, v. not. L. Le Fur, « Les caractère essentiels du droit en comparaison avec les autres règles de la vie sociale », *Archives de philosophie du droit et de sociologie juridique* 1935, p. 7. Pour un bref exposé des rapports entre sanction et effectivité, v. not. Y. Leroy, « La notion d'effectivité du droit », *Droit et société* 2011, n° 79, p. 715, spéc. p. 722 s.

[1165] V. not. N. Martial-Braz, J. Rochfeld et E. Gattone, « Quel avenir pour la protection des données à caractère personnel en Europe ? Les enjeux de l'élaboration chaotique du règlement 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 », *D.* 2013, p. 2788.

[1166] J. Rivero, « Sur l'effet dissuasif de la sanction juridique », in *Mélanges P. Raynaud*, Dalloz, 1985, p. 675 s.

[1167] E. Netter, *Numérique et grandes notions du droit privé. La personne, la propriété, le contrat*, mémoire en vue de l'habilitation à diriger des recherches en droit privé, Picardie, 20 nov. 2017, n° 68, p. 91. V. aussi, É. Gabrié, « Les pouvoirs des autorités de protection des données », *Dalloz IP/IT* 2017, p. 268.

[1168] Pour un bref panorama des missions de la CNIL, E. Delisle, « Le nouveau rôle de la CNIL », *Jurisport* 2019, n° 196, p. 32. Pour une présentation plus approfondie des missions de la CNIL, *JCl. administratif,* fasc. 274-50, « Informatique – Commission nationale de l'informatique et des libertés », par R. Perray, 2019 (actu. 2020), n°s 42 s.

[1169] G. Desgens-Pasanau, « Contrôles et sanctions de la CNIL : quelles évolutions ? », *CCE* 2018, n° 4, dossier 17.

élevé entre ces deux méthodes de calcul étant retenu[1170]. Un tel système de sanction a tendance à transformer le droit des données à caractère personnel en un droit répressif, le rapprochant ainsi du régime de protection de la vie privée.

321. Le rapprochement avec le régime de protection de la vie privée. Depuis l'adoption de ses premières règles, le droit des données personnelles a largement évolué. La loi du 6 janvier 1978 fondait son régime sur une distinction organique entre les traitements opérés par le secteur public et ceux mis en œuvre par le secteur privé[1171]. La directive européenne 95/46 a acté l'abandon de cette distinction en droit français et a assoupli les obligations déclaratives. Quant au règlement européen, il a mis fin à la plupart des obligations déclaratives et organisé un principe de responsabilité. Les passages successifs d'un système formaliste fondé sur un critère organique, à un système formaliste fondé sur un critère qualitatif, puis à un système de responsabilisation actent le glissement d'un système préventif vers un système répressif. Cette évolution rapproche le régime de données à caractère personnel du droit au respect de la vie privée, garanti par l'article 9 du code civil[1172].

Cet article avait été adopté notamment pour mettre fin à la dérive jurisprudentielle en matière de responsabilité civile qui s'était progressivement adaptée aux particularités du droit au respect de la vie privée[1173]. Si, dans un premier temps, la jurisprudence appliqua le triptyque traditionnel (un fait générateur, un dommage et un lien de causalité) de manière classique, elle procéda rapidement à certains assouplissements[1174]. Lorsque les juges étaient saisis sur le fondement de l'ancien article 1382 du code civil, ils avaient pris l'habitude d'adapter ces conditions à la spécificité des atteintes à la vie privée. Le seul fait de raconter la vie privée d'une personne sans son consentement est progressivement considéré comme une faute[1175], et les demandes sont accueillies même lorsque le préjudice n'est pas complètement

---

[1170] Art. 83 du règlement UE n° 2016/679.
[1171] V. *supra,* n^{os} 305 s.
[1172] Article issu de la loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens, *JORF* 19 juill. 1970, n° 0166, p. 6755.
[1173] P. Jourdain, « Les droits de la personnalité à la recherche d'un modèle : la responsabilité civile », *Gaz. Pal.* 2007, n° 139, p. 52. Sur l'évolution de la responsabilité civile en matière de droit au respect de la vie privée, D. Chauvet, *La vie privée. Étude de droit privé,* th. Paris-Sud, 2014, n^{os} 371 s., p. 313 s.
[1174] T. Azzi, « Les relations entre la responsabilité civile délictuelle et les droits subjectifs », *RTD civ.* 2007, p. 227, n° 8.
[1175] F. Terré et D. Fenouillet, *Droit civil. Les personnes*, 8^{e} éd., Dalloz, 2012, n° 108, p. 118. Pour Pierre Kayser, commet une faute celui qui ne se comporte pas de façon normale, honnête ou avisée, P. Kayser, *La protection de la vie privée par le droit*, 3^{e} éd., Economica, 1995, n° 66, p. 118 et n° 196, p. 364.

établi[1176]. De sorte que les conditions de la responsabilité étaient présumées dès qu'une personne apportait la preuve d'une atteinte à sa vie privée[1177]. Pour éviter de poursuivre cette entorse aux conditions classiques de la responsabilité civile délictuelle, le législateur français a consacré un arsenal juridique répressif permettant au juge d'intervenir non seulement pour prévenir la réalisation d'une telle atteinte (notamment dans le cadre du référé)[1178], mais surtout pour la réparer lorsqu'elle s'est produite. L'article 9 du code civil organise donc un régime répressif dans lequel la seule constatation de l'atteinte à la vie privée ouvre droit à réparation[1179]. Si cet article prévoit également des dispositions propres à prévenir ces atteintes, le siège de la matière réside dans ses mesures réparatrices[1180].

À l'origine, la loi du 6 janvier 1978 complétait très bien l'arsenal législatif du droit au respect de la vie privée puisque les obligations déclaratives permettaient un contrôle en aval des atteintes aux personnes. Comme le remarquait Pascal Ancel, le principal intérêt de la loi de 1978 résidait dans ses dispositions préventives[1181]. Les mesures préventives attiraient l'attention du déclarant sur les dangers potentiels de son traitement, l'encourageant à la prudence. Le glissement progressif du droit des données personnelles vers un régime de plus en plus répressif tend à faire se superposer toutes ces règles et à complexifier leur articulation[1182].

Dans tous les cas, pour être licites, les traitements de données à caractère personnel doivent être fondés sur une condition de licéité.

[1176] CA Paris, 17 mars 1966, *J.-L. Trintignant*, *D.* 1966, p. 749, v. aussi la note signée P. A. et H. M. ss. CA Paris, 15 mai 1970, *Jean Ferrat*, *D.* 1970, p. 466.
[1177] P. Jourdain, « Les droits de la personnalité à la recherche d'un modèle : la responsabilité civile », *Gaz. Pal.* 2007, n° 139, p. 52.
[1178] *Rép. civ.* Dalloz, *V°* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), n° 221.
[1179] Cass. civ. 1re, 5 nov. 1996, n° 94-14.798, *Bull. civ.* 1996, I, n° 378, p. 265. V. not. P. Roubier, « Délimitation et intérêts pratiques de la catégorie des droits subjectifs », *Archives de philosophie du droit* 1964, t. 9, p. 83, spéc. p. 94 ; P. Kayser, « Le secret de la vie privée et la jurisprudence civile », in *Mélanges R. Savatier*, Dalloz, 1965, p. 405 s., n° 2, spéc. p. 406.
[1180] *Rép. civ.* Dalloz, *V°* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), nos 249 s.
[1181] P. Ancel, « La protection des données personnelles : aspects de droit privé français », *RID comp.* 1987, vol. 39, n° 3, p. 609, spéc. p. 618. V. *supra*, n° 218.
[1182] D'ailleurs, les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques sont soumis, en vertu de l'article 35 du règlement UE n° 2016/679, à une analyse d'impact. Une telle obligation inclut la plupart des traitements portant atteinte au respect de la vie privée des personnes. D'ailleurs, la CNIL fait explicitement référence à l'atteinte à la vie privée dans sa présentation de l'analyse d'impact relative à la protection des données, v. CNIL, « Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données (AIPD) », 22 oct. 2019.

SOUS-SECTION II – LA MULTIPLICITÉ DES CONDITIONS LÉGITIMANT LES TRAITEMENTS

322. Plan. Le droit des données à caractère personnel impose aux responsables du traitement de justifier leurs traitements de données. Pour cela, ils peuvent avoir recours à une ou plusieurs conditions de licéité (§ I). Sous une apparente rigidité, ces conditions de licéité sont finalement assez accommodantes (§ II).

§ I. Présentation des conditions de licéité

323. Plan. Après avoir étudié la montée en puissance de la place des conditions de licéité en droit des données personnelles (A), nous exposerons les six conditions de licéité permettant de justifier les traitements de données à caractère personnel (B).

A. Justification de l'existence des conditions de licéité

324. L'obligation de justifier l'atteinte. En France, jusqu'à 2004, seuls les traitements de données sensibles devaient être fondés sur une justification[1183]. Pour les autres traitements, le responsable du traitement devait simplement respecter ses obligations déclaratives, informer les personnes concernées du caractère obligatoire ou facultatif de leurs réponses, des conséquences d'un défaut de réponse, et leur offrir un droit d'opposition[1184].

La directive 95/46 a introduit l'obligation de fonder les traitements sur une justification, c'est-à-dire l'obligation de justifier les traitements. Cette obligation illustre la volonté du législateur d'encourager les responsables du traitement à s'interroger sur les motivations qui les poussent à collecter des données, notamment dans le but de mieux encadrer les atteintes aux personnes.

L'article 7 de la directive 95/46 prévoyait que tout traitement de données personnelles n'était légitime que dans deux cas de figure : soit la personne avait indubitablement donné son consentement, soit le traitement répondait à une finalité indiquée parmi une liste de cinq alternatives : le traitement était nécessaire à

[1183] L'article 31 de la loi nº 78-17 du 6 janvier 1978 prévoyait l'obligation de recueillir l'accord exprès de la personne concernée pour ces traitements.
[1184] Art. 27 de la loi nº 78-17 du 6 janv. 1978. Comme le remarque Madame Anne Debet au sujet de la loi du 6 janvier 1978, « ce texte, comme la Convention 108 du Conseil de l'Europe, ne se posait tout simplement pas la question de la nécessité d'un fondement du traitement », v. A. Debet, « Le consentement dans le RGPD : rôle et définition », *CCE* 2018, nº 4, dossier 9.

l'exécution d'un contrat ou de mesures précontractuelles, au respect d'une obligation légale, à la sauvegarde de l'intérêt vital de la personne, à l'exécution d'une mission d'intérêt public, ou à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement[1185]. Lorsque l'une de ces six conditions était présente, la loi établissait une sorte de présomption de licéité du traitement. Monsieur Dany Cohen remarquait, à juste titre, que les dérogations prévues par la liste des alternatives au consentement permettaient de légitimer d'avance « l'écrasante majorité des traitements de données, car mises bout à bout ces hypothèses ouvrent un champ de licéité immense »[1186].

325. Les conditions de licéité du traitement dans le règlement. Le règlement européen a repris ces conditions en élevant leur niveau d'exigence conceptuel, en leur apportant quelques précisions[1187] et en supprimant leur caractère alternatif[1188]. Désormais, un responsable du traitement peut donc fonder ses traitements sur six fondements de licéité différents[1189]. Toutes ces conditions de licéité ne sont pas basées sur le même intérêt : certaines d'entre elles sont en rapport avec la personne concernée, alors que d'autres se fondent sur un intérêt extérieur.

Cette mise en balance entre l'intérêt de la personne concernée et un intérêt extérieur n'est pas inconnue du droit civil puisqu'elle se retrouve notamment dans la jurisprudence fondée sur l'article 9 du code civil. Dans sa thèse sur la vie privée, Madame Delphine Chauvet exposait deux types d'intérêts permettant de justifier une atteinte à la vie privée : l'intérêt particulier et l'intérêt général[1190]. Elle distinguait ces intérêts du consentement de la personne qui, lui, « neutralise » la protection de la vie

---

[1185] Article 7 de la directive CE nº 95/46 transposé dans l'article 7 de la loi nº 78-17 du 6 janvier 1978 telle que modifiée par la loi nº 2004-801 du 6 août 2004.
[1186] D. Cohen, « Le juge européen et les données personnelles », in *Mélanges R. Badinter*, Dalloz, 2016, p. 249 s., spéc. p. 255.
[1187] N. Métallinos, « Les apports du règlement général relatif à la protection des données personnelles sur les conditions de licéité des traitements », *Dalloz IP/IT* 2016, p. 588.
[1188] L'article 6 du règlement UE nº 2016/679 prévoit ainsi 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; 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. »
[1189] C'est d'ailleurs ce que fait Facebook qui fonde ses traitements de données à caractère personnel sur les six conditions, Facebook, « Sur quel fondement juridique nous appuyons-nous pour traiter les données ? En savoir plus », consulté le 29 oct. 2020.
[1190] D. Chauvet, *La vie privée. Étude de droit privé,* th. Paris-Sud, 2014, nºs 568 s., p. 437 s.

privée[1191]. Selon elle, « la mise en œuvre du droit au respect de la vie privée suppose que la personne n'a pas volontairement permis une intrusion dans sa vie privée »[1192]. Ainsi, la volonté de la personne anéantit la protection de la vie privée alors qu'elle n'a pas d'influence sur la mise en œuvre de la protection des données[1193]. Le consentement de la personne concernée est donc mis sur un pied d'égalité avec les intérêts extérieurs pouvant rendre légitime un traitement de données. Quelle que soit la condition de licéité, les droits et obligations qui découlent de ce traitement sont les mêmes pour le responsable du traitement.

B. Exposé des conditions de licéité

326. Les deux fondements liés à la volonté de la personne concernée. Seules deux des six conditions de licéité sont en rapport avec la volonté de la personne concernée[1194]. Il s'agit de la condition du contrat et de celle du consentement. Le consentement étant classiquement défini comme un « accord de deux ou plusieurs volontés en vue de créer des effets de droit ; ou la « rencontre de ces volontés qui est la condition de la formation du contrat »[1195], d'importants rapprochements sont à prévoir entre ces deux conditions qui feront l'objet de développements postérieurs[1196]. Une autre condition autorise le traitement dans l'*intérêt* de la personne concernée. Il s'agit des traitements de données personnelles nécessaires à la sauvegarde de ses intérêts vitaux[1197]. Ces conditions témoignent de la place relative de la personne concernée dans la décision de traiter ses données personnelles. En l'absence de volonté, ou même pour contrecarrer un éventuel refus de traitement, d'autres fondements peuvent être utilisés pour traiter les données à caractère personnel.

[1191] Selon l'auteur, « logiquement, quand la personne consent à l'investigation ou à la divulgation de sa vie privée, la protection de celle-ci n'a pas lieu d'être mise en œuvre », D. Chauvet, *La vie privée. Étude de droit privé,* th. Paris-Sud, 2014, n^os^ 479 s, spéc. n^o^ 482, p. 380 s.
[1192] D. Chauvet, *La vie privée. Étude de droit privé,* th. Paris-Sud, 2014, n^os^ 479 s, p. 380 s. V. dans le même sens pour le secret des correspondances, V. Peltier, *Le secret des correspondances,* th. Aix-Marseille, 1998, PUAM, n^o^ 518, p. 401 s.
[1193] CEPD, Guidelines 05/2020 on consent under Regulation 2016/679, 4 mai 2020, § 5, p. 5.
[1194] Le G29 parle d'autodétermination de la personne concernée pour justifier le traitement, v. G29, WP 217, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, 9 avr. 2014, p. 14.
[1195] G. Cornu (dir.), *Vocabulaire juridique*, 13^e^ éd., PUF, 2020, *V^o^* « Consentement », sens 1.
[1196] V. *infra*, n^os^ 338 s.
[1197] Art. 6 §1 d) du règlement UE n^o^ 2016/679. Cette disposition distingue deux types d'intérêts vitaux : ceux de la personne concernée et ceux d'une autre personne physique. Dans la même idée, le droit médical prévoit une dérogation au principe d'obtention du consentement, notamment lorsque le patient est hors d'état d'exprimer sa volonté, v. M. Le Goues, *Le consentement du patient en droit de la santé*, th. Perpignan, 2015, p. 184 s.

327. Les quatre fondements liés à un intérêt extérieur. Quatre des six conditions sont basées sur un intérêt extérieur à la personne concernée : le traitement des données personnelles effectué pour le respect d'une obligation légale, pour l'exécution d'une mission de service public, pour la sauvegarde des intérêts vitaux d'une autre personne physique et pour la poursuite d'intérêts légitimes. Ces fondements révèlent l'existence d'un contrôle de proportionnalité effectué en amont par le législateur. En effet, il s'agit bien d'une mise en balance entre d'un côté la protection des données personnelles (caractérisée par le pouvoir de contrôle de la personne sur ses données) et de l'autre, la liberté de circulation de l'information, l'intérêt général ou la liberté d'entreprendre. Le législateur a donc instauré une forme de contrôle de proportionnalité *in abstracto,* établissant une présomption de licéité des traitements. Évidemment, cette présomption simple ne suffit pas à garantir la conformité au droit des données personnelles, mais elle dénote une vision favorable à la mise en œuvre des traitements de données personnelles.

328. Les traitements fondés sur l'intérêt général. Parmi les quatre conditions permettant de justifier le traitement par un intérêt extérieur à la personne concernée, deux sont fondées sur l'intérêt général. Les contours et le contenu de la notion d'intérêt général sont délicats à cerner, et Demogue remarquait que l'intérêt général ne serait « qu'une expression commode » dont « il faut se défier »[1198].

Malgré ces difficultés, le Conseil constitutionnel a recours à cette notion pour justifier une intervention de la puissance publique réductrice de certains droits ou libertés individuelles appelés à céder devant les impératifs collectifs[1199]. C'est ce qui explique que la doctrine fait valoir que « l'intérêt général est reconnu par la plupart des textes relatifs aux droits fondamentaux comme une limite nécessaire à la mise en œuvre des droits pour qu'ils ne deviennent pas une source d'abus de l'individu »[1200].

Dans le domaine des données personnelles, l'intérêt général permet de contourner la volonté des personnes concernées. L'intérêt général se matérialise dans

---

[1198] R. Demogue, *Les notions fondamentales du droit privé*, LGDJ, 1911, p. 175.
[1199] N. Lenoir, « Table-ronde », in *Colloque l'intérêt général, norme constitutionnelle ?,* dir. B. Mathieu et M. Verpeaux, Dalloz, 2006, p. 82. Le Vocabulaire juridique de l'Association Henri Capitant définit l'intérêt public et général comme « ce qui est pour le bien public, à l'avantage de tous », v. G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vo* « Intérêt », sens 2.
[1200] X. Bioy, *Droits fondamentaux et libertés publiques*, 5e éd., LGDJ, 2018, n° 485, p. 240. L'auteur n'hésite pas à rappeler le caractère central de la notion d'intérêt général, mais aussi les difficultés liées à son appréhension. Il remarque d'ailleurs que l'intérêt général « ne se définit pas, il se proclame et se désigne ».

la condition de l'obligation légale et celle de l'exécution d'une mission d'intérêt public. En effet, l'adoption d'une disposition légale suppose une mise en balance par le législateur de l'intérêt des individus à la protection de leurs données et de celui de la société. Dans cette appréciation, le législateur conclut alors à la prévalence de l'intérêt de la société sur l'intérêt personnel[1201]. Il en est ainsi par exemple de la mise en œuvre des traitements de données par les services des impôts[1202]. Quant à la mission d'intérêt public, elle concerne principalement les traitements mis en œuvre par les autorités publiques ou les organismes privés chargés d'une mission d'intérêt public, c'est-à-dire les organismes investis d'une mission de service public[1203]. La notion de service public renvoie directement à l'idée d'intérêt général[1204]. La CNIL a précisé par exemple que les laboratoires pratiquant des analyses ADN sur demande de l'autorité judiciaire à partir d'échantillons biologiques prélevés sur les scènes d'infractions ou auprès de personnes mises en cause dans des affaires judiciaires étaient investis d'une telle mission de service public[1205]. Ici encore, c'est donc l'intérêt général qui rend légitime la mise en œuvre des traitements de données personnelles, et ce, en dehors de toute volonté de la personne concernée. Cette condition laisse une grande marge d'interprétation aux organismes et pourrait, en l'absence de contrôle[1206], faire l'objet d'abus.

329. Les traitements fondés sur un intérêt particulier. Deux conditions de licéité rendent légitime un traitement de données grâce à un intérêt particulier extérieur à celui de la personne concernée. Il s'agit d'une part des intérêts légitimes, lesquels feront l'objet d'une étude spécifique[1207], et d'autre part de la sauvegarde des intérêts vitaux d'une personne. Cette condition a été étendue par le règlement européen, puisque désormais les intérêts vitaux d'une *autre* personne physique que ceux de la personne concernée peuvent justifier un traitement de données personnelles[1208]. Cette condition

---

[1201] L'article 6 § 3 du règlement UE nº 2016/679 précise que ces obligations sont définies soit par le droit de l'Union soit par celui de l'État membre auquel le responsable du traitement est soumis.
[1202] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 635, p. 267 s.
[1203] CNIL, « La mission d'intérêt public : dans quels cas fonder un traitement sur cette base légale ? », 2 déc. 2019.
[1204] J. Waline, *Droit administratif,* 28e éd., Dalloz, 2020, nº 33, p. 23.
[1205] CNIL, délibération nº 2012-408 du 22 novembre 2012 portant avis sur un projet de décret en Conseil d'État relatif à la mise en œuvre de traitements de données à caractère personnel dénommés « outils de recherche de contamination ADN » (ORCA).
[1206] Sur l'importance des contrôles dans le système actuel, v. *supra*, nº 320.
[1207] V. *infra*, nºs 333 s.
[1208] La directive 95/46 faisait seulement référence, dans son article 7 d) à « la sauvegarde de l'intérêt vital de la personne concernée ».

doit être mise en perspective avec celle prévue pour les traitements de données sensibles, autorisés « lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement »[1209]. Ainsi, le législateur européen considère, à juste titre, que la sauvegarde des intérêts vitaux d'une personne tierce prévaut, par principe, sur la volonté de la personne concernée. Une telle primauté semble parfaitement justifiée dès lors que l'intérêt mis en balance avec le traitement de données personnelles est une vie humaine.

Ainsi, pour ces quatre conditions, c'est bien une mise en balance entre la protection des données personnelles et la protection d'intérêts extérieurs à la personne concernée qui est opérée en amont par le législateur[1210]. En plus de ces conditions, d'autres intérêts rendent également légitimes certains traitements de données.

330. La mise en balance des intérêts par les responsables du traitement. Aux fondements juridiques permettant de traiter des données personnelles s'ajoutent, depuis 1995, l'ensemble des exceptions et régimes spéciaux permettant de déroger aux principes de protection. Alors qu'elles étaient originellement dispersées au fil de la directive, le règlement européen a regroupé ces dérogations dans le chapitre IX, tout en déclarant dès le considérant 4 que « le présent règlement respecte tous les droits fondamentaux et observe les libertés et les principes reconnus par la Charte, consacrés par les traités ». Parmi ces exceptions figurent par exemple les traitements effectués dans le cadre de la liberté d'expression et d'information[1211], les traitements effectués à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques[1212], ou encore les traitements justifiés par l'accès du public aux documents officiels[1213].

Pour certaines de ces libertés, le législateur européen a renvoyé aux États membres le soin d'organiser les dérogations et exemptions nécessaires pour assurer un équilibre entre la protection des données et ces libertés[1214]. Ces renvois créent une

---

[1209] Art. 9 du règlement UE nº 2016/679. Sur le consentement en droit médical, v. M. Le Goues, *Le consentement du patient en droit de la santé*, th. Perpignan, 2015, p. 184 s.
[1210] L. Bygrave et D. Wiese Schartum, « Consent, proportionnality and collective power », in *Reinventing Data Protection*, dir. S. Gutwirth, P. De Hert, S. Nouwt, Y. Poullet et C. de Terwangne, Springer, 2009, p. 157.
[1211] Art. 85 du règlement UE nº 2016/679.
[1212] Art. 89 du règlement UE nº 2016/679.
[1213] Art. 86 du règlement UE nº 2016/679.
[1214] Pour une critique de la prétendue « conciliation » entre ces libertés, v. R. Post, « Tensions entre "droit au débat public" et "droit au déréférencement". Regard d'outre-Atlantique », *RID comp.* 2017, nº 4, p. 821, spéc. p. 835.

fragmentation territoriale dans l'application des règles de protection, contraire à l'objectif d'uniformisation du règlement européen[1215].

Ces exceptions, bien que justifiées et nécessaires dans une société démocratique, sont une illustration supplémentaire de la souplesse des règles organisant les traitements de données personnelles.

331. Des règles favorables aux traitements. Pour résumer, parmi les six fondements permettant de rendre licites les traitements de données personnelles, seuls deux d'entre eux sont en rapport avec la volonté de la personne concernée. Les quatre autres sont liés à des intérêts extérieurs. En plus de ces intérêts extérieurs permettant de justifier les traitements, les dérogations prévues par le règlement européen accentuent encore le contrôle très relatif des personnes à l'égard de leurs données[1216]. L'ensemble de ce système présente donc des risques pour l'effectivité de la protection des personnes. L'analyse détaillée de trois de ces conditions de licéité conforte ce sentiment.

§ II. Des conditions de licéité accommodantes

332. Plan. Parmi les six conditions de licéité, certaines se révèlent favorables à la mise en place des traitements. Cela se vérifie particulièrement pour la condition fondée sur les intérêts légitimes (A) et, dans une moindre mesure, pour les conditions liées à la volonté de la personne (B).

A. La condition liée aux intérêts légitimes

333. L'intérêt légitime, une condition souple. À première vue, la notion d'intérêt légitime est imprécise et laisse une grande place à l'interprétation[1217]. La directive de 1995 n'avait d'ailleurs pas détaillé ses contours, ni explicité les types d'intérêts

---

[1215] Cet objectif d'uniformisation est souvent présenté par la Commission européenne comme achevé, v. par ex. V. Jourovà, « Why US needs to get tough on privacy. Europe is leading the way with new regulations and wants Washington to join in », *Politico* 11 avr. 2019. Pourtant, le règlement européen est émaillé de quelques 56 renvois aux droits nationaux, v. A.-Y. Le Dain et P. Gosselin, « Rapport d'information sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française », Assemblée nationale, n° 4544, 22 févr. 2017, annexe n° 1. Pour une analyse des difficultés liées aux renvois opérés par le règlement européen, M.-É. Ancel, « D'une diversité à l'autre. A propos de la "marge de manœuvre" laissée par le règlement général sur la protection des données aux États membres », *Revue critique de droit international privé* 2019, p. 647.

[1216] M. Boizard, « Données à caractère personnel – Le consentement à l'exploitation des données à caractère personnel : une douce illusion ? », *CCE* 2016, n° 3, étude 6.

[1217] F. Rigaux, « Libre circulation des données et protection de la vie privée dans l'espace européen », in *La protection de la vie privée dans la société d'information*, t. 2, dir. P. Tabatoni, PUF, 2002, p. 35. V. aussi, A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, n^os^ 645 s., p. 268 s.

légitimes pouvant être invoqués. Le caractère ouvert de cette condition a suscité d'importantes débats quant à sa portée et son application. La doctrine a vu dans cette condition un véritable « cheval de Troie »[1218], et Guy Braibant s'était inquiété de la voir justifier, à terme, la majorité des traitements du secteur privé[1219]. En pratique, les intérêts pouvant être invoqués sur ce fondement semblent très variés. Le G29 retient d'ailleurs une définition large de l'intérêt légitime puisqu'il considère qu'il s'agit de « l'enjeu poursuivi par le responsable du traitement, ou le bénéfice qu'il tire du traitement »[1220]. La Cour de justice de l'Union européenne a ainsi pu affirmer que l'intérêt économique de l'exploitant d'un moteur de recherche (c'est-à-dire la volonté de tirer profit de l'exploitation des données personnelles de ses utilisateurs) pouvait être considéré comme un intérêt légitime au sens de la directive 95/46[1221]. Il semble donc que la seule limite à cet intérêt est qu'il ne soit… pas illégitime ! C'est sans doute ce qui amenait le G29 a rappelé que ce critère « est parfois perçu à tort comme une "porte ouverte" légitimant tout traitement de données qui ne cadre avec aucun autre fondement juridique », et qu'il a permis à des personnes « de s'y référer automatiquement ou d'en élargir indûment l'utilisation au prétexte qu'il semble moins contraignant que les autres motifs »[1222].

334. Le fondement dans le règlement européen. Dans le règlement européen, les intérêts légitimes au pluriel remplacent l'intérêt légitime au singulier. Cette extension renforce encore davantage la perception que ce critère est une commodité laissée aux organismes pour fonder la licéité de leurs traitements. D'autant que l'article étend aussi les intérêts des tiers pris en compte puisque si la directive visait expressément certains tiers (les tiers auxquels les données sont communiquées), le règlement européen vise désormais, et de manière évasive, « un tiers »[1223]. En apparence, cette condition accueille donc les intérêts d'un plus grand nombre de personnes. Sans doute, ces

---

[1218] N. Martial-Braz, J. Rochfeld et E. Gattone, « Quel avenir pour la protection des données à caractère personnel en Europe ? Les enjeux de l'élaboration chaotique du règlement 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 », *D.* 2013, p. 2788.
[1219] G. Braibant, « Données personnelles et société de l'information. Rapport au Premier ministre sur la transposition en droit français de la directive nº 95/46 », La Documentation française, 1998, p. 55.
[1220] G29, WP 217, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, 9 avr. 2014, p. 55.
[1221] La Cour a toutefois considéré que ce seul intérêt économique ne permet pas de justifier un traitement susceptible d'affecter significativement les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, CJUE, 13 mai 2014, *Google Spain SL, Google Inc.* c. *Agencia Española de Protección de Datos, Mario Costeja González,* C-131/12, § 80 s.
[1222] G29, WP 217, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, 9 avr. 2014, p. 5 et p. 55.
[1223] Art. 6 § 1 f) du règlement UE nº 2016/679.

intérêts devront quand même avoir un lien suffisamment important avec le responsable du traitement pour qu'ils lui permettent de justifier son traitement.

335. Les intérêts légitimes, un fondement de mise en balance. Pour éviter une application trop permissive de ce fondement, le législateur impose au responsable du traitement de mettre en balance les intérêts légitimes avec l'intérêt ou les libertés et droits fondamentaux de la personne concernée[1224]. Le règlement européen a clarifié les intérêts à prendre en compte dans cette mise en balance puisqu'il indique désormais que *tous* les intérêts ou libertés et droits fondamentaux de la personne concernée doivent être pris en considération et non plus seulement ceux prévus par l'article 1er de la directive de 1995. Il insiste également sur l'importance de la protection des enfants. Pour qu'un traitement de données à caractère personnel puisse valablement se fonder sur les intérêts légitimes, deux conditions cumulatives doivent donc être vérifiées. D'une part, le traitement doit être nécessaire à la réalisation des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, et d'autre part, les droits et libertés fondamentaux de la personne concernée ne doivent pas prévaloir sur ces intérêts[1225]. Le résultat de cette mise en balance détermine, dans une large mesure, si ce fondement justifie le traitement.

336. Un fondement malléable. Bien que le considérant 47 du règlement européen donne quelques exemples de situations dans lesquelles les intérêts légitimes pourraient valablement être invoqués, notamment lorsqu'il existe une relation contractuelle entre la personne concernée et le responsable du traitement, l'appréciation *in concreto* revient au responsable du traitement. En effet, il est le seul capable de faire la mise en balance entre ses intérêts légitimes et les droits et libertés des personnes concernées, sans que celles-ci soient en capacité de la vérifier.

Pour preuve, l'entreprise Facebook déclare dans sa politique de confidentialité, sans plus de précision, se fonder sur ses « intérêts légitimes ou ceux d'un tiers » pour

---

[1224] G29, WP 217, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, 9 avr. 2014, p. 26. Dans son article 7, la directive CE nº 95/46 prévoyait que l'intérêt légitime peut être invoqué, « à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er paragraphe 1 ». Étaient ainsi visés les seuls droits et libertés fondamentaux protégés par l'article 1er de ce texte, c'est-à-dire « la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel ».

[1225] V. déjà CJUE, 24 nov. 2011, *ASNEF et FECEMD* c. *Administración del Estado,* C-468/10 et C-469/10, § 38.

justifier le traitement de données collectées afin de « promouvoir les produits des entités Facebook et lancer notre marketing direct » ou encore « dans l'intérêt des annonceurs, développeurs et autres partenaires, pour les aider à comprendre leurs clients et à améliorer leurs affaires, à valider nos modèles de tarification et à évaluer l'efficacité de leur contenu en ligne et de leur publicité sur les produits des entités Facebook et ailleurs »[1226]. Facebook déclare également traiter des données personnelles sur le fondement de l'intérêt légitime pour « améliorer les connaissances actuelles et la connaissance académique des questions sociales importantes afin de changer notre société et le monde de manière positive »[1227]. Ces déclarations particulièrement vagues et imprécises ne permettent pas à la personne concernée de vérifier concrètement comment ses droits et libertés ont été mis en balance avec les intérêts de Facebook et des tiers.

Certains auteurs ne manquent pas de rappeler que « l'intérêt légitime du responsable de traitement doit être invoqué avec une grande prudence, car il requiert une mise en balance avec les droits de la personne concernée. Les résultats d'une telle pesée ne sont pas faciles à prévoir, et les analyses de la CNIL peuvent diverger de celles du responsable de traitement au moment du contrôle, et il est alors trop tard »[1228]. Le faible nombre de contrôles de la conformité de ce critère dans le traitement mis en œuvre remet en cause l'effectivité de la protection des personnes.

337. Peu de contrôles de l'application de ce fondement. L'imprécision notionnelle, cumulée au pouvoir unilatéral accordé à l'organisme, confirme que ce fondement est un véritable « cheval de Troie » pour la protection des données personnelles. Il est donc impératif que des contrôles soient plus systématiques afin d'éviter un dévoiement de ce fondement. À ce titre, il est surprenant de constater que cette disposition est peu présente dans les décisions de la CNIL, hormis dans les délibérations relatives aux dispositifs d'alerte professionnelle[1229]. Pourtant, la CNIL aurait pu cibler ses contrôles

[1226] La politique de confidentialité ne détaille pas les intérêts du tiers pris en compte pour justifier le traitement, Facebook, « Sur quel fondement juridique nous appuyons-nous pour traiter les données ? En savoir plus », consulté le 29 oct. 2020.
[1227] Facebook, « Sur quel fondement juridique nous appuyons-nous pour traiter les données ? En savoir plus », consulté le 29 oct. 2020.
[1228] E. Netter, « Sanction à 50 millions d'euros : au-delà de Google, la CNIL s'attaque aux politiques de confidentialité obscures et aux consentements creux », *Dalloz IP/IT* 2019, p. 165.
[1229] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 648, p. 271.

à l'égard des organismes fondant leurs traitements sur cette condition[1230], notamment pour vérifier la mise en balance entre les intérêts[1231]. La jurisprudence judiciaire et administrative est, elle aussi, peu développée en la matière[1232]. Des contrôles plus systématiques doivent donc être organisés pour conjurer les possibles détournements de ce fondement et éviter de rendre légitimes, au moins en apparence, tous les traitements.

B. Les conditions liées à la volonté de la personne

338. Plan. Au sein des conditions de licéité fondés sur la volonté de la personne concernée, le droit des données personnelles opère une distinction entre le consentement et le contrat. Celle-ci a sans doute été jugée nécessaire du fait de l'absence de reconnaissance, dans le droit de certains États membres, de la catégorie des contrats unilatéraux. En pratique, l'expression d'un consentement annonce souvent l'existence d'un contrat. L'articulation entre ces deux fondements risque donc de présenter certaines difficultés. Après avoir identifié ces difficultés (1), une proposition d'articulation doit être formulée (2). Celle-ci se caractérise par la reconnaissance d'un contrat spécial au traitement de donnée à caractère personnel (3). Une telle reconnaissance emporte certaines conséquences (4).

1. Difficultés d'articulation

339. Le consentement dans la directive. En apparence, la directive 95/46 attribuait au consentement une position prépondérante puisque celui-ci était placé en tête des conditions de licéité ; les autres fondements étaient de simples alternatives lorsque le

---

[1230] D'ailleurs, à l'occasion des débats parlementaires de transposition de la directive CE n° 95/46, les rapporteurs des deux assemblées avaient rappelé l'exigence d'un contrôle *a priori* et *a posteriori* de la CNIL sur ces questions, v. G. Gouzes, « Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », Assemblée nationale, n° 3526, 9 janv. 2002, p. 35 ; A. Türk, « Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », Sénat, n° 218, 19 mars 2003, p. 58.

[1231] Les analyses de l'autorité peuvent diverger de celles retenues par le responsable du traitement, v. par ex. CNIL, décision n° 2013-025 du 10 juin 2013 de la Présidente de la Commission nationale de l'informatique et des libertés mettant en demeure la société Google Inc. et CNIL, délibération n° 2013-420 du 3 janvier 2014 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google Inc.

[1232] Selon les auteurs du manuel *Informatique et libertés,* les juridictions administratives n'auraient fait référence à cette condition « qu'une fois et les juridictions judiciaires ne l'ont fait que très rarement et de manière succincte », A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, n^{os} 652 s., p. 274. Par exemple, la cour d'appel de Paris, dans un arrêt relativement médiatisé (*Note2be*) concernant un site de notation des enseignant du secondaire, avait été saisie de la question de savoir si l'intérêt lucratif de l'entreprise suffisait à conférer un intérêt légitime au traitement lui-même. Sans répondre directement à cette question, la juridiction constatait que l'équilibre entre les droits des enseignants et celui des personnes pouvant les noter n'était pas respecté et ordonnait des mesures de suspension du site, v. CA Paris, 14^{e} ch., 25 juin 2008, *Note2be.com* c. *SNES FSU et autres*, n° 08/04727.

consentement ne pouvait pas être obtenu. Selon certains auteurs, le consentement serait d'ailleurs la condition cardinale du régime de traitement des données[1233]. D'autres auteurs relativisent toutefois cette affirmation et rappellent qu'il n'est pas le fondement prioritaire des traitements et qu'il n'est pas forcément le plus adapté[1234]. Le G29, le CEPD et la CNIL ont récemment confirmé cette interprétation stricte de la condition du consentement et ont encouragé les organismes à s'assurer que cette condition était la plus même de répondre aux spécificités du traitement[1235].

340. Le consentement et le contrat. Le plus souvent, l'expression de la volonté se matérialise juridiquement par le consentement qui apparaît comme « l'élément fondamental de tout contrat »[1236]. En définissant le contrat comme « un accord de volontés entre deux ou plusieurs personnes destiné à créer, modifier, transmettre ou éteindre des obligations », l'article 1101 du code civil accorde effectivement une place centrale au consentement : sans consentement, il n'est pas de contrat[1237]. C'est pourquoi la rencontre de consentements prédit souvent l'existence d'un contrat[1238]. D'ailleurs, selon une opinion doctrinale, le consentement prévu par le droit des données personnelles ne serait qu'une étape vers l'élaboration d'un contrat. Ainsi, l'inscription au service et l'acceptation de ses conditions générales caractérisent la rencontre des volontés[1239]. Pour Monsieur Benjamin Charrier, par exemple, lorsque les mineurs utilisent les réseaux sociaux, ils expriment « un consentement au sens du droit des

---

[1233] C. Castets-Renard, « Brève analyse du règlement général relatif à la protection des données personnelles », *Dalloz IP/IT* 2016, p. 331.
[1234] A. Debet, « Le consentement dans le RGPD : rôle et définition », *CCE* 2018, n° 4, dossier 9.
[1235] V. not. G29, WP 187, Avis 15/2011 relatif à la définition du consentement, 13 juill. 2011, p. 7 ; G29, WP 259 rév. 01, Lignes directrices sur le consentement au sens du règlement 2016/679, 10 avr. 2018, p. 4 ; CEPD, Guidelines 05/2020 on consent under Regulation 2016/679, 4 mai 2020, § 2 s., p. 5. V. aussi CNIL, délibération n° 2012-214 du 19 juillet 2012 portant avertissement à l'encontre de la société FNAC.
[1236] P. Malinvaud, M. Mekki et J.-B. Seube, *Droit des obligations*, 15e éd., LexisNexis, 2019, n° 126, p.120.
[1237] F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, n° 78, p. 88. Pour les besoins de notre démonstration, nous considérons que les termes de consentement et de volonté sont synonymes. Pour autant, d'autres auteurs considèrent qu'il faut distinguer ces deux termes, v. not. M.-A. Frison-Roche, « Remarques sur la distinction de la volonté et du consentement en droit des contrats », *RTD civ.* 1995, p. 575.
[1238] C. Larroumet et S. Bros, *Traité de droit civil. Les obligations, le contrat*, t. 3, 9e éd., Economica, 2018, n° 226, p. 200.
[1239] Pour Monsieur Grégoire Loiseau, « l'intégration des conditions générales d'utilisation dans le champ contractuel et, subséquemment, leur contractualisation par l'inscription au réseau social, sont difficilement contestables », G. Loiseau, « La valeur contractuelle des conditions générales d'utilisation des réseaux sociaux », *CCE* 2012, n° 7-8, comm. 78. E. Netter, « L'extinction du contrat et le sort des données personnelles », *AJ Contrat* 2019, p. 416. Pour une analyse détaillée de l'interaction entre le consentement et les conditions générales, v. F. Limbach, *Le consentement contractuel à l'épreuve des conditions générales des contrats : de l'utilité du concept de la déclaration de volonté*, th. Toulouse I et Université de la Sarre, 2003, LGDJ.

contrats, puisqu'il faut rappeler que nous sommes ici bien en présence de contrats »[1240]. Selon ces auteurs, le consentement au traitement des données à caractère personnel n'est donc que l'une des étapes nécessaires à la formation du contrat[1241]. À l'inverse, une autre opinion doctrinale considère qu'il faut distinguer ces deux conditions, lesquelles seraient indépendantes. Ainsi, pour Monsieur Thibault Douville, il conviendrait de différencier « le consentement donné au traitement, manifestation de volonté par laquelle la personne concernée autorise le traitement de ses données qui s'analyse comme un acte juridique unilatéral, et le consentement au contrat »[1242]. Malheureusement, ce type d'affirmations n'aide pas à déterminer la nature du contrat auquel la personne consent. Elles ne permettent pas non plus d'identifier les éléments qui distinguent le consentement à l'acte juridique unilatéral du consentement au contrat.

La doctrine est donc divisée sur les conséquences de la qualification du consentement au traitement de données personnelles. Pourtant, cette qualification est très importante dans la mesure où les règles applicables au consentement au traitement de données personnelles sont substantiellement plus contraignantes que celles applicables au consentement d'un contrat de droit commun. Ainsi, un responsable du traitement pourrait fonder son traitement sur le contrat et échapper aux règles plus contraignantes applicables au consentement. Cette dualité soulève donc d'importantes difficultés qu'il convient d'examiner en détail.

341. Les problèmes de cette dualité. Le fait que le droit des données personnelles reconnaisse deux fondements juridiques dont les critères d'application sont en pratique très similaires, engendre des problèmes dans la mise en œuvre des traitements, la sécurité juridique et l'articulation entre ces deux fondements. Il interroge surtout sur l'opportunité d'un tel cumul. En effet, le contrat est, par essence, la rencontre de deux volontés matérialisées par des consentements, et il est parfois difficile de déceler ce qui distingue le consentement à un traitement de données personnelles d'un contrat

---

[1240] B. Charrier, « Le consentement exprimé par les mineurs en ligne », *Dalloz IP/IT* 2018, p. 333. Cette affirmation efface la distinction posée par l'article 6 du règlement européen entre le consentement et le contrat et se place purement d'un point de vue contractuel.

[1241] C'est d'ailleurs le sens du point 4 de l'article 7 du règlement européen qui prévoit que « Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat ».

[1242] T. Douville, « La protection des données à caractère personnel des mineurs et des majeurs protégés », *RLDC* 2018, nº 162, p. 42, § 9.

portant sur un traitement de telles données[1243]. La doctrine pointe, à juste titre, les incohérences que ces deux fondements créent, en questionnant notamment l'utilité de l'exigence d'un consentement renforcé lorsqu'il est possible de la contourner dans l'hypothèse d'une relation contractuelle[1244]. Par exemple, l'entreprise Facebook considère que le fondement principal de ses traitements est le contrat et n'a recours au consentement que dans des cas résiduels, alors même qu'il semblerait qu'un nombre important des traitements effectués par le réseau social devraient être fondés sur le consentement de la personne concernée[1245]. Si le CEPD considère que « ces deux bases juridiques du traitement de données à caractère personnel (…) ne peuvent pas être fusionnées et amalgamées »[1246], leur articulation demeure complexe et engendre des conséquences réelles pour la protection des personnes.

342. Les conséquences pratiques de cette superposition. La difficulté d'articulation entre ces deux fondements n'est pas seulement théorique. Elle a des applications pratiques importantes puisqu'un traitement pourra être déclaré illicite si son fondement n'est pas valable. Cette difficulté était d'ailleurs au cœur de l'avertissement prononcé par la CNIL à l'égard de la FNAC en 2012, dans lequel était contestée la pratique de l'entreprise consistant à enregistrer par défaut, et sans consentement particulier, les données de cartes bancaires de ses clients en vue de futures transactions[1247]. La question était ici de savoir quel fondement de licéité pouvait justifier la conservation de ces données de cartes bancaires. La société invoquait la nécessité contractuelle et l'intérêt légitime pour soutenir qu'elle n'avait pas à obtenir un consentement spécifique. La CNIL rejette cette interprétation en considérant que la

---

[1243] S. Pellet, « RGPD : l'effacement du consentement », *RGDA* 2019, nº 1, p. 6.
[1244] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nos 640 s., p. 268. Malgré plusieurs avis sur le consentement et le contrat, le groupe des autorités européennes de contrôle n'a jamais analysé en profondeur les interactions entre le consentement prévu par le droit des données à caractère personnel et celui prévu par le droit commun des contrats. Par exemple, dans son avis de 2019 sur le contrat, le CEPD prétend régler les interactions entre le contrat et le consentement par ces affirmations laconiques : « lorsque le traitement n'est pas considéré comme "nécessaire à l'exécution d'un contrat", c'est-à-dire lorsqu'un service demandé peut être fourni sans que le traitement spécifique ait lieu, le CEPD reconnaît qu'une autre base juridique peut être applicable, pour autant que les conditions pertinentes soient remplies. En particulier, dans certaines circonstances, il peut être plus approprié de se fonder sur le consentement donné librement », CEPD, Lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées, 8 oct. 2019, § 17, p. 7.
[1245] Il est possible de supposer que de nombreuses données collectées par Facebook ne sont pas liées au contrat conclu entre l'utilisateur du service et le réseau social. En effet, les données que l'entreprise collecte ne sont pas nécessaires pour la prestation de réseau social entendu comme un site mettant en relation des utilisateurs en ligne. Par exemple, les données collectées pour la publicité ciblée effectuée par l'entreprise ne servent pas cet objectif du réseau social mais serve un intérêt autre (celui de monétiser la vente des espaces publicitaires).
[1246] CEPD, Guidelines 05/2020 on consent under Regulation 2016/679, 4 mai 2020, § 26, p. 10.
[1247] CNIL, délibération nº 2012-214 du 19 juillet 2012 portant avertissement à l'encontre de la société FNAC.

FNAC devait obtenir un consentement spécifique au traitement des données de cartes bancaires, parce que la fonctionnalité de portefeuille électronique était distincte de celle liée au contrat de vente en ligne. La CNIL ne précise pas la nature de la relation nouée entre la personne concernée et l'organisme, à la suite de l'expression de ce consentement au traitement des données de cartes bancaires. Pourtant, la nature de cette relation peut avoir des effets importants sur le choix du fondement de licéité. En effet, quelle est la nature de la relation établie entre le responsable du traitement qui propose un traitement de données personnelles et la personne concernée acceptant cette proposition ? Selon Monsieur Emmanuel Netter, le document décrivant les modalités de traitement engage l'organisme et doit donc s'analyser comme une pollicitation. Quant au consentement de la personne concernée, il doit être considéré comme une acceptation, permettant la création d'un contrat[1248]. Dès l'instant où cette relation est qualifiée de contractuelle, l'organisme ne pourrait-il pas fonder son traitement sur la condition du contrat et ainsi contourner les exigences de consentement renforcé prévues par le droit des données personnelles ? Cette difficulté révèle une nouvelle possibilité pour les organismes de mettre en œuvre leurs traitements en contournant les règles protectrices du droit des données personnelles, réduisant ainsi l'effectivité de cette protection. Pour mettre fin aux difficultés d'articulation entre ces deux fondements, une proposition doit être formulée.

2. *Proposition d'articulation : la reconnaissance d'un contrat spécial de traitement de données à caractère personnel*

343. L'identification d'un contrat portant sur le traitement de données personnelles. Pour déterminer si la relation qui se crée entre la personne acceptant le traitement de ses données et l'organisme qui effectue ce traitement a une nature contractuelle, il faut savoir si un contrat a pu se former. Dans cette détermination, il convient dans un premier temps de rappeler les conditions de formation du contrat pour ensuite s'interroger sur leur réunion lorsque la personne concernée émet un consentement au traitement de ses données.

[1248] E. Netter, « L'extinction du contrat et le sort des données personnelles », *AJ Contrat* 2019, p. 416.

344. L'existence d'un contrat. Le contrat est souvent défini comme un accord de volontés entre deux ou plusieurs personnes destiné à produire des effets de droit[1249]. La volonté est donc le moteur des actes juridiques[1250], et l'accord de volontés, le cœur du contrat[1251].

345. La définition du consentement. Pris dans son sens étymologique, le mot consentement (*cum sentire*) désigne *l'accord*[1252] et le verbe consentir signifie « être de même sentiment » ou « être d'accord »[1253]. Le contrat est donc une expression de volonté visant à acquiescer à quelque chose. Lorsque le consentement est envisagé sous l'angle juridique, le droit des contrats s'impose assez naturellement. Bien sûr, le consentement se retrouve dans d'autres domaines du droit, notamment en procédure pénale[1254], mais c'est en droit des contrats qu'il occupe une place aussi centrale.

En matière contractuelle, le terme « consentement » revêt une double acceptation[1255]. Il désigne d'abord la manifestation de volonté de chacune des parties, c'est-à-dire l'acquiescement que celles-ci donnent aux conditions du contrat projeté. Il désigne également l'accord de volonté qui fait naître une volonté nouvelle[1256].

346. Un acte juridique unilatéral ? Avant de s'intéresser aux obligations résultant de ces volontés, il convient de se demander si le consentement au traitement de données à caractère personnel ne serait pas plutôt un acte juridique unilatéral[1257]. Ce dernier est classiquement défini comme la manifestation de volonté par laquelle une personne,

---

[1249] Selon Madame Judith Rochfeld, « l'approche "classique" du contrat, qui reposait sur l'article 1101 du code civil précité, le présentait comme ne créant que des obligations, c'est-à-dire des contraintes précises, ayant pour objet une prestation déterminée, d'essence plutôt économique, au profit d'un créancier identifié. Or, au-delà de ces obligations, des auteurs se sont attachés à renouveler l'analyse et à démontrer que le contrat donnait également naissance à d'autres types d'effets, relevant davantage d'une norme juridique », J. Rochfeld, *Les grandes notions du droit privé*, 2e éd., PUF, 2013, *Vo* « Le contrat », no 13, p. 436. V. par ex. P. Ancel, « Force obligatoire et contenu obligationnel », *RTD civ.* 1999, p. 771 ; S. Lequette, « La notion de contrat », *RTD civ.* 2018, p. 541 ; B. Moron-Puech, « De quelques faiblesses de la définition traditionnelle du contrat », *Droits* 2017, p. 115 s. ; D. Galbois, *La notion de contrat. Esquisse d'une théorie*, th. Paris II, 2018.

[1250] J. Carbonnier, *Droit civil,* t. 4, *Les obligations*, 22e éd., PUF, 1996, no 14, p. 48.

[1251] P. Malaurie, L. Aynès et P. Stoffel-Munck, *Les obligations*, 10e éd., LGDJ, 2018, no 454, p. 254. V. également, J. Ghestin, G. Loiseau et Y.-M. Serinet, *La formation du contrat*, 4e éd., 2013, no 198, p. 157.

[1252] F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, no 145, p. 182.

[1253] F. Gaffiot, *Dictionnaire Latin-Français*, Hachette, 2000, *Vo* « Consentīre », sens I.1.

[1254] V. par ex. V. Antoine, *Le consentement en procédure pénale*, th. Montpellier, 2011.

[1255] F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, nos 145 s, p.182 s.

[1256] G. Rouhette, *Contribution à l'étude critique de la notion de contrat*, th. Paris, 1965, no 98 s., p. 364 s.

[1257] Il s'agissait d'ailleurs de la qualification retenue par Monsieur Thibault Douville, T. Douville, « La protection des données à caractère personnel des mineurs et des majeurs protégés », *RLDC* 2018, no 162, p. 42, § 9.

agissant seule, détermine des effets de droit[1258]. Ainsi, pour savoir si le consentement au traitement de données à caractère personnel est un acte juridique unilatéral, il faut vérifier qu'en agissant seule, la personne concernée crée des effets de droit. La principale limite à cette qualification se trouve dans le fait que la personne concernée n'agit pas « seule ». Elle agit selon un cadre proposé par le responsable du traitement et pour lequel elle accepte de s'engager. Le responsable du traitement occupe une place essentielle dans la détermination des conditions du traitement accepté par la personne. Ainsi, le consentement exprimé au traitement de données à caractère personnel se caractérise donc plutôt par une rencontre de volontés que par un acte juridique unilatéral.

347. L'échange des consentements. Aux termes de l'article 1113 du code civil, « le contrat est formé par la rencontre d'une offre et d'une acceptation par lesquelles les parties manifestent leur volonté de s'engager ». L'offre désigne, selon l'article 1114 du code civil, la proposition de conclure un contrat à des conditions déterminées, de telle sorte que son acceptation suffit à la formation de celui-ci. Elle doit donc contenir tous les éléments permettant de définir précisément l'objet du contrat, notamment pour pouvoir l'exécuter[1259]. Il convient donc de se demander si la proposition du responsable du traitement peut être qualifiée d'offre, au sens du droit des contrats.

En vertu du considérant 42 du règlement européen, le responsable du traitement doit exposer les finalités du traitement auquel sont destinées les données à caractère personnel. Le CEPD précise d'ailleurs que le responsable du traitement doit énoncer non seulement la finalité de chacune des opérations de traitement pour lesquelles le consentement est sollicité, mais aussi les types de données collectées et utilisées[1260]. Le responsable du traitement doit donc expliquer la façon dont il compte traiter les données[1261]. À ce titre, une information succincte et compréhensible doit être fournie à la personne concernée ; les développements juridiques peuvent, quant à eux, être

---

[1258] J. Flour, J.-L. Aubert et E. Savaux, *Droit civil. Les obligations.* t. 1, *L'acte juridique,* 16e éd., Sirey, 2014, no 489, p. 502 ; F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, no 509, p. 591.

[1259] M. Fabre-Magnan, *Droit des obligations,* t. 1, *Contrat et engagement unilatéral*, 5e éd., PUF, 2019, no 410, p. 327.

[1260] CEPD, Guidelines 05/2020 on consent under Regulation 2016/679, 4 mai 2020, § 64, p. 15.

[1261] Ainsi, en droit des données à caractère personnel, le législateur encadre fortement les conditions dans lesquelles la rencontre des volontés s'opère. Par exemple, le législateur impose au responsable du traitements des obligations d'information. Cet interventionnisme s'inscrit dans une tendance plus générale, sur les contrats forcés, v. F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, nos 46 s., p. 48 ; P. Malinvaud, M. Mekki et J.-B. Seube, *Droit des obligations*, 15e éd., LexisNexis, 2019, no 127, p.121.

consignés dans une politique de confidentialité[1262]. L'exposé des conditions du traitement sont fermes et précises, elles caractérisent donc les éléments d'une offre au sens du droit des contrats.

L'acceptation résulte de l'agrément pur et simple de l'offre par le destinataire de celle-ci[1263]. Sur Internet, beaucoup d'offres sont faites au public[1264], et les personnes sont invitées à accepter purement et simplement la proposition de service[1265]. En cliquant sur le bouton « j'accepte », la personne donne son accord pur et simple au traitement proposé par l'organisme. Une acceptation semble donc caractérisée au sens du droit des contrats. Plusieurs formulations du règlement européen font d'ailleurs écho à la notion d'acceptation en droit des contrats. Par exemple, le considérant 32 du règlement européen affirme que le consentement de la personne concernée désigne « son accord au traitement des données à caractère personnel ». De manière plus explicite encore, ce considérant prévoit que la personne concernée « *accepte* le traitement *proposé* de ses données à caractère personnel »[1266].

Ainsi, la proposition de traitement formulée par le responsable du traitement revêt les caractères d'une offre au sens du droit des contrats et le consentement exprimé par la personne concernée a les caractéristiques d'une acceptation, permettant ainsi la rencontre des volontés.

348. La volonté de s'engager juridiquement. Pour que l'accord de volonté soit qualifié juridiquement comme un contrat, encore faut-il que les parties aient eu l'intention de s'obliger[1267], ou à tout le moins, dans une approche moins subjective, que la création de tels effets de droit soit reconnue par l'ordre juridique[1268]. Selon une

---

[1262] V. not. art. 12 du règlement UE nº 2016/679.
[1263] F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, nº 183, p. 213.
[1264] Sur les contrats entre absents et les contrats par Internet, v. C. Larroumet et S. Bros, *Traité de droit civil. Les obligations, le contrat*, t. 3, 9e éd., Economica, 2018, nº 280 p. 247.
[1265] Il est fréquent que le détail de l'offre soit énoncé dans des conditions générales d'utilisation ou des politiques de confidentialité. En 2010, à l'occasion du 1er avril, l'ancien site de vente de jeux vidéo GameStation avait ajouté une clause dans ses conditions de vente prévoyant que l'acheteur acceptait d'octroyer à l'entreprise une option lui permettant de lui réclamer son âme. Les clients avaient accepté cette proposition en acceptant, sans lire, les conditions générales de vente, P. Garoscio, « Lisez les conditions d'utilisation ou vous finirez par laver des toilettes », *clubic.com* 22 juill. 2017.
[1266] Une formulation similaire se retrouve également dans le considérant 42 du règlement UE nº 679/2016.
[1267] M. Fabre-Magnan, *Droit des obligations,* t. 1, *Contrat et engagement unilatéral*, 5e éd., PUF, 2019, nº 229, p. 198.
[1268] Une opinion doctrinale moderne a renouvelé l'analyse classique du contrat pour montrer que celui-ci donnait également naissance à d'autres types d'effets, relevant davantage d'une norme juridique, v. P. Ancel, « Force obligatoire et contenu obligationnel », *RTD civ.* 1999, p. 771 ; S. Lequette, « La notion de contrat », *RTD civ.* 2018, p. 541 ; B. Moron-Puech, « De quelques faiblesses de la définition traditionnelle du contrat », *Droits* 2017, p. 115 s. ; D. Galbois, *La notion de contrat. Esquisse d'une théorie*, th. Paris II, 2018.

définition classique, l'obligation est un « lien de droit existant entre deux personnes et en vertu duquel l'une (le créancier) est en droit d'exiger quelque chose de l'autre (le débiteur) »[1269]. Dans le cadre d'un contrat dont l'objet serait le traitement de données à caractère personnel, la question de la nature des obligations des deux parties se pose[1270].

D'un côté, l'obligation du responsable du traitement est relativement facile à identifier. Celui-ci s'engage à faire ou à ne pas faire un certain nombre de choses (fournir un service spécifique, faciliter les achats ultérieurs en conservant les données de cartes bancaires, transmettre les données à des partenaires commerciaux, etc.). Il s'engage donc à traiter les données pour certaines finalités et dans certaines conditions.

De l'autre côté, l'obligation de la personne concernée est, à première vue, plus difficile à déterminer. Il est certain qu'elle souhaite s'engager dans un rapport d'obligations avec l'organisme puisqu'elle veut bénéficier de la prestation proposée[1271]. Son obligation pourrait éventuellement être qualifiée d'obligation de *praestare*, c'est-à-dire l'obligation pour la personne de mettre à disposition ses données à caractère personnel[1272]. Toutefois, une telle obligation est difficilement concevable dès lors que le fait de disposer de ses données à caractère personnel est une liberté fondamentale et que la personne concernée ne peut se voir contrainte au traitement de ses données que dans de rares cas[1273].

Une autre hypothèse pourrait être que la personne concernée s'engage à une obligation de ne pas faire. Comme le remarquait Monsieur Grégoire Loiseau à propos du contrat autorisant l'usage du patronyme, l'auteur de l'autorisation s'engage à une obligation de ne pas exercer son droit à la protection du patronyme, ce dernier devant alors être entendu comme le droit d'exclure un tiers de son utilisation[1274]. Une telle

---

[1269] J. Flour, J.-L. Aubert et E. Savaux, *Droit civil. Les obligations,* t. 1, *L'acte juridique,* 16e éd., Sirey, 2014, no 8, p. 6.

[1270] Sur les obligations liées aux droits de la personnalité, v. déjà, P. Kayser, « Le secret de la vie privée et la jurisprudence civile », in *Mélanges R. Savatier*, Dalloz, 1965, p. 405 s., nos 8 s., spéc. p. 413 s.

[1271] Pour que cet engagement soit considéré comme valable, la personne doit pouvoir exercer un choix véritable sans sentir de contrainte ou subir des conséquences négatives importantes, v. cons. 42 du règlement UE no 679/2016.

[1272] D. Chauvet, *La vie privée. Étude de droit privé,* th. Paris-Sud, 2014, no 196, p. 166 s. Plusieurs auteurs complètent cette classification par l'obligation de *praestare*, venant de *præstō* devant être traduit, selon le dictionnaire Gaffiot, par « sous la main » ou « à la disposition », F. Gaffiot, *Dictionnaire Latin-Français*, Hachette, 2000, *Vo* « Præstō », sens 1 et 2. Il s'agit de l'obligation de mise à disposition temporaire de l'usage d'une chose, v. J. Huet, « Des différentes sortes d'obligations et plus particulièrement de l'obligation de donner, la mal nommée, la mal aimée », *Mélanges J. Ghestin*, 2001, p. 425 s., no 4, spéc. p. 428.

[1273] Notamment lorsque l'intérêt général le requiert comme c'est le cas pour les traitements de données mis en œuvre par des administrations, tels que les impôts.

[1274] G. Loiseau, *Le nom, objet d'un contrat*, th. Paris I, 1995, LGDJ, nos 301 s., p. 289 s. ; v. aussi, I. Tricot-Chamard, *Contribution à l'étude des droits de la personnalité. L'influence de la télévision sur la conception*

conception est transposable en matière de données à caractère personnel : l'obligation de la personne concernée consiste à autoriser l'organisme à traiter ses données à caractère personnel[1275]. Celui-ci obtient ainsi la possibilité d'utiliser licitement les données personnelles, et c'est la bascule de l'illicite vers le licite qui constitue l'effet principal, ainsi que les obligations du responsable du traitement.

Le responsable du traitement et la personne concernée partagent donc la volonté de créer des obligations : l'une d'elles s'engage à accorder l'usage de certaines de ses données tandis que l'autre s'engage à traiter ces données selon certaines conditions. À première vue, il est donc possible de considérer qu'un contrat est né à la suite de cette rencontre de volonté. Pour être valable, ce contrat devra toutefois répondre à certaines conditions.

349. Les conditions nécessaires à la validité du contrat. L'article 1128 du code civil pose trois conditions à la validité du contrat : le consentement, la capacité des parties à contracter et le contenu licite et certain du contrat. Les deux premières conditions font l'objet de dispositions spécifiques en matière de consentement au traitement de données personnelles que nous étudierons plus avant[1276]. La troisième condition, relative au contenu du contrat, mérite quant à elle certains développements préliminaires, puisque la possibilité de contracter sur des éléments de la personnalité a longtemps fait l'objet de débats.

350. Le contrat portant sur une obligation extrapatrimoniale. L'obligation est classiquement définie comme un lien de droit entre deux personnes par lequel l'une est tenue à une prestation à l'égard de l'autre[1277]. Il en résulte que l'obligation a longtemps été présentée comme un rapport de droit entre deux patrimoines[1278]. Cette présentation était confortée par l'intitulé du livre III du code civil – « Des différentes manières dont on acquiert la propriété » – dans lequel figure, avec d'autres matières, les obligations. Toutefois les définitions plus récentes des obligations ne manquent pas de remarquer

---

juridique de la personnalité, th. Paris I, 2004, PUAM, n° 105, p. 100. Plus largement sur les droits de la personnalité, v. B. Teyssié, *Droit des personnes*, 21e éd., LexisNexis, 2019, n° 262, p. 236.

[1275] Sur l'autorisation comme l'octroi d'une faculté, v. B. Thullier, *L'autorisation. Étude de droit privé*, th. Paris X, 1993, LGDJ, nos 65 s.

[1276] V. *infra,* nos 358 s.

[1277] J. Carbonnier, *Droit civil,* vol. 2, *Les biens. Les obligations*, PUF, 2004, n° 922, p. 1917.

[1278] C. Larroumet et S. Bros, *Traité de droit civil, Les obligations. Le contrat*, t. 3, 9e éd., Economica, 2018, n° 22, p. 18. En droit italien, la patrimonialité est l'essence de l'obligation, v. R. Sacco, « À la recherche de l'origine de l'obligation », *Archives de philosophie du droit* 2000, t. 44, p. 33, spéc. p. 38.

le caractère réducteur de cette vision[1279]. Comme le notait déjà Jhering, certaines des clauses du contrat, voire tout le contrat, peuvent prévoir des obligations purement personnelles sans conséquence sur le patrimoine des cocontractants[1280]. Ainsi, le droit des contrats intéresse également les obligations extrapatrimoniales dont l'objet n'est pas toujours la satisfaction des intérêts économiques et pécuniaires du créancier[1281]. Des droits extrapatrimoniaux peuvent donc être l'objet de contrat. Par exemple, un contrat peut porter sur la liberté d'expression (matérialisée par l'obligation de confidentialité), la liberté de travailler (organisée par des clauses de non-concurrence) ou sur l'organisation de la vie commune des partenaires (présente dans le Pacte civil de solidarité)[1282]. Le contenu d'un contrat peut donc être de nature extrapatrimoniale. Pour autant, il reste classique d'affirmer que la personne humaine est indisponible et son corps hors du commerce juridique[1283]. Qu'en est-il de ses informations personnelles ?

351. Les contrats sur les droits de la personnalité. Les droits de la personnalité sont définis comme les droits attachés à la personne humaine qui appartiennent de droit à toute personne physique et sans valeur patrimoniale directe[1284]. L'idée exprimée en 1909 par Perreau selon laquelle les droits de la personnalité sont non seulement incessibles, mais plus généralement hors du commerce, et donc insusceptibles de conventions, a profondément marqué la tradition juridique française[1285]. Une telle affirmation est d'ailleurs confortée par certains principes fondamentaux du droit,

---

[1279] V. not. M. Fabre-Magnan, *Droit des obligations,* t. 1, *Contrat et engagement unilatéral*, 5e éd., PUF, 2019, no 3, p. 3.
[1280] R. Von Jhering, « De l'intérêt dans les contrats, et de la prétendue nécessité de la valeur patrimoniale des prestations obligatoires », dans *Œuvres choisies*, vol. II, Librairie A. Marescq, 1893, p. 145 s. V. aussi, M. Fabre-Magnan, *Droit des obligations,* t. 1, *Contrat et engagement unilatéral*, 5e éd., PUF, 2019, no 296, p. 237.
[1281] F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, no 4, p. 4.
[1282] B. Morre, « Contrat et religion. À la volonté de Dieu ou des contractants ? Commentaire sur l'affaire *Marcovitz c. Bruker* », *Revue juridique Thémis* 2009, vol. 43, p. 219 s. [43 R.J.T. 219] spéc. p. 234. Sur le contrat de travail, v. A. Supiot, *Le juge et le droit du travail,* th. Bordeaux I, 1979.
[1283] R. Demogue, *Traité des obligations en général,* t. 2, Librairie Arthur Rousseau, 1923, no 803, p. 652 ; F. Terré et P. Simler, *Droit civil. Les biens*, 10e éd., Dalloz, 2018, no 14, p. 20 s. ; G. Loiseau, « Le rôle de la volonté dans le régime de protection de la personne et de son corps », *McGill Law Journal* 1992, vol. 37, no 4, p. 965 s. [37 McGill L.J. 965], spéc. p. 966. Comp. C. Labrusse-Riou, « De quelques apports du droit des contrats au droit des personnes », in *Mélanges J. Ghestin*, LGDJ, 2001, p. 499 s., spéc. p. 500.
[1284] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vo* « Personnalité », sens 2. Plus largement, v. Y. Buffelan-Lanore et V. Larribau-Terneyre, *Droit civil. Introduction, biens, personnes, famille,* 21e éd., Sirey, 2019, no 132, p. 63 ; F. Terré et D. Fenouillet, *La famille,* 8e éd., Dalloz, 2012, no 5, p. 4. Comp. P. Ancel, *L'indisponibilité des droits de la personnalité. Une étude critique des droits de la personnalité,* th. Dijon, 1978.
[1285] E.-H. Perreau, « Des droits de la personnalité », *RTD civ.* 1909, p. 501, spéc. p. 517. L'auteur nuançait tout de même son propos en affirmant que « rigoureusement parlant, les droits de la personnalité, placés hors du commerce, sont (…) hors des atteintes de la volonté humaine. Ceci, c'est de la théorie ; mais en pratique, rien n'eût été plus fâcheux. Aussi, les tribunaux ont-ils largement atténué cette idée ».

notamment les articles 6[1286], 16-1 alinéa 3[1287] et 16-5[1288] du code civil qui protègent la personne et son corps. D'une manière générale, il était difficilement concevable que la personne, sujet de droit, participe de l'objet d'un contrat et se retrouve tout à la fois sujet et objet de droit[1289]. Ainsi, de prime abord, les droits de la personnalité paraissent devoir être rangés parmi les choses hors commerce[1290].

Toutefois, cette conception est aujourd'hui obsolète, tant le nombre de contrats portant sur ces droits a explosé[1291]. En effet, on assiste depuis le milieu du XX[e] siècle à la multiplication de ces contrats, notamment les conventions relatives à l'usage du nom[1292], à l'exploitation de l'image[1293] ou aux traitements d'informations personnelles[1294]. À cela s'ajoute également le concept d'autonomie personnelle développé par la Cour européenne des droits de l'homme qui est appréhendé comme la possibilité reconnue au sujet de poser sa propre norme et de décider pour soi-même[1295]. C'est pourquoi les auteurs s'accordent désormais pour considérer que la réalité ne peut être résumée à un pur principe d'indisponibilité des droits de la personnalité[1296]. La conception actuelle veut que tant qu'un acte ne menace pas l'impératif de protection

---

[1286] Lequel dispose qu'on « ne peut déroger, par des conventions particulières, aux lois qui intéressent l'ordre public et les bonnes mœurs ».
[1287] Lequel dispose que le « corps humain, ses éléments et ses produits ne peuvent faire l'objet d'un droit patrimonial ».
[1288] Lequel dispose que les « conventions ayant pour effet de conférer une valeur patrimoniale au corps humain, à ses éléments ou à ses produits sont nulles ».
[1289] M. Bourgeois, *La personne objet de contrat*, th. Paris I, 2003, Paradigme, n° 2, p. 4.
[1290] F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, n° 509, p. 591.
[1291] C. Filippone, *La contractualisation des droits de la personnalité,* th. Paris I, 2001 ; A.-A. Hyde, *Les atteintes aux libertés individuelles par contrat. Contribution à la théorie de l'obligation,* th. Paris I, 2015, IRJS, n° 676, p. 471. Pour une distinction entre les choses hors commerce et les choses hors du marché, G. Loiseau, « Typologie des choses hors du commerce », *RTD civ.* 2000, p. 47.
[1292] Sur le nom comme objet de contrat, v. déjà en 1910, E.-H. Perreau, *Le droit au nom en matière civile*, Sirey, 1910, p. 143 s. ; plus récemment v. G. Loiseau, *Le nom, objet d'un contrat*, th. Paris I, 1995, LGDJ. En jurisprudence, v. not. Cass. com., 12 mars 1985, n° 84-17.163, *Bull.* 1985, IV, n° 95, p. 84.
[1293] Sur l'image de la personne comme objet de contrat, v. J. Ravanas, *La protection des personnes contre la réalisation et la publication de leur image*, th. Aix-en-Provence, 1978, LGDJ, nos 387 s., p. 435 ; M. Serna, *L'image et le droit*, th. Paris II, 1994, Economica, p. 24 ; M. Bourgeois, *La personne objet de contrat*, th. Paris I, 2003, Paradigme, nos 103 s., p. 193 s. ; C. Deschanel, *Le droit patrimonial à l'image : émergence d'un nouveau droit voisin du droit d'auteur*, th. Avignon, 2017, nos 423 s., p. 261 s. En jurisprudence, v. not. Cass. civ. 1re, 11 déc. 2008, n° 07-19.494, *Bull. civ.* 2008, I, n° 282.
[1294] F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, n° 509, p. 591. V. aussi, J. Rochfeld, « Une nouvelle source en droit des contrats : la loi Informatique et libertés », *RDC* 2014, n° 1, p. 119, § 4.
[1295] Sur cette protection, voir la jurisprudence particulièrement développée de la CEDH, not. CEDH, 29 avr. 2002, *Pretty* c. *Royaume-Uni*, n° 2346/02, § 61. Sur ce concept, M. Levinet, « La notion d'autonomie personnelle dans la jurisprudence de la cour européenne des droits de l'homme », *Droits* 2009, n° 49, p. 3.
[1296] P. Ancel, *L'indisponibilité des droits de la personnalité. Une étude critique des droits de la personnalité,* th. Dijon, 1978, n° 187, p. 188. V. plus réc. G. Loiseau, « La crise existentielle du droit patrimonial à l'image », *D.* 2010, p. 450 ; *Rép. civ.* Dalloz, *Vo* « Inaliénabilité », par R.-N. Schütz, 2014 (actu. 2019), n° 36 ; R. Ollard, « Qualification de droits extrapatrimoniaux », in *Droits de la personnalité,* dir. J.-C. Saint-Pau, LexisNexis, 2013, n° 560, p. 338.

de la personne, notamment le principe de dignité, il doit être permis et ne pas tomber sous le coup de l'indisponibilité[1297].

352. Les contrats sur le traitement de données personnelles. Le droit des données à caractère personnel figure parmi les droits de la personnalité[1298]. Plusieurs auteurs remarquent d'ailleurs que ce droit est d'autant plus nécessaire que les développements technologiques ont accru les risques d'atteinte aux personnes[1299]. Comme les autres droits de la personnalité, les données à caractère personnel peuvent donc faire l'objet de contrats.

353. L'opération de qualification. Afin de différencier un « simple » contrat d'un contrat portant sur le traitement de données à caractère personnel, il convient de procéder à une opération de qualification. Plusieurs méthodes existent pour qualifier un contrat, mais c'est souvent la recherche de sa *prestation caractéristique* qui permet d'en déterminer sa nature[1300].

Dans certains cas, le contrat peut avoir pour *objet principal* le traitement de données à caractère personnel, c'est-à-dire que le contenu du contrat a trait par exemple à la collecte, l'analyse, l'exploitation, la communication, ou l'interconnexion de données à caractère personnel[1301]. C'est notamment le cas lorsque la personne accepte le dépôt de cookies à l'occasion de la visite d'un site Internet ou qu'elle accepte la conservation de ses données bancaires pour des transactions futures. Dans ces situations, la prestation caractéristique du contrat est le traitement de données à

[1297] M. Bourgeois, *La personne objet de contrat*, th. Paris I, 2003, Paradigme, n° 102, p. 193. V. not. J. Hauser, « L'indisponibilité relative des droits de la personnalité : conventions directes et indirectes sur le droit au respect de la vie privée et le droit au secret », *RTD civ.* 2000, p. 801 ; G. Loiseau, « La contractualisation des droits de la personnalité », *JCP G* 2012, n° 4, note 71.

[1298] *Rép. civ.* Dalloz, *V°* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), n° 31. Selon Madame Murielle Bénéjat, « les droits sur les données personnelles font l'objet de plusieurs qualifications. La qualification de droit de la personnalité s'impose d'emblée. Comment les droits sur sa propre identité pourraient-ils ne pas être, conformément à la définition doctrinale consacrée, "inhérents à la seule qualité de la personne humaine" et ainsi "appartenir à tout individu par le fait même qu'il est homme" ? », M. Bénéjat, « Les droits sur les données personnelles », in *Droits de la personnalité,* dir. J.-C. Saint-Pau, LexisNexis, 2013, n° 926, p. 561.

[1299] A. Marais, *Droits des personnes*, 3e éd., Dalloz, 2018, n° 234, p. 159 ; L. Marino, « Les nouveaux territoires des droits de la personnalité », *Gaz. Pal.* 2007, n° 139, p. 22.

[1300] D. Mainguy, *Contrats spéciaux*, 11e éd., Dalloz, 2018, n° 15, p. 30. Sur la question de la qualification en matière contractuelle, v. F. Terré, *De l'influence de la volonté individuelle sur les qualifications,* th. Paris, 1955, LGDJ, réimpr. 2014 ; X. Henry, *La technique de qualifications contractuelles,* th. Nancy II, 1992.

[1301] La définition posée par l'article 4 § 2 du règlement UE inclut l'ensemble de ces opérations et n'est pas limitative. Pour une analyse détaillée de cette notion, v. not. O. Tambou, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, nos 80 s., p. 72 s. ; M. Bourgeois, *Droit de la donnée. Principes théoriques et approche pratique,* LexisNexis, 2017, nos 122 s., p. 37 s.

caractère personnel. Le contrat devra donc être qualifié de *contrat de traitement de données personnelles*.

Au contraire, lorsque l'objet principal du contrat requiert, pour sa formation ou son exécution, la collecte de données à caractère personnel, mais que celle-ci est nécessaire pour l'exécution d'une autre prestation, le contrat devra être considéré comme soumis aux règles du droit commun des contrats[1302]. En effet, dans ces situations, le traitement des données est encadré par l'interprétation stricte de la condition de nécessité[1303]. Le CEPD a d'ailleurs rappelé que la nécessité d'un traitement doit être interprétée objectivement et ne peut être une simple clause contractuelle[1304] C'est le cas, par exemple, pour l'abonnement à un journal : l'éditeur du journal perçoit le paiement en échange de quoi l'abonné reçoit les journaux. Le traitement de certaines des données personnelles de l'abonné (telles que son nom et son adresse) est nécessaire à la livraison des journaux puisque, sans ce traitement, l'éditeur ne pourrait pas exécuter son obligation de délivrance des journaux. En revanche, si l'éditeur du journal venait à traiter ces données pour d'autres finalités (telles que la publicité pour des produits de la marque ou d'annonceurs), il devrait alors fonder son traitement sur une autre condition (sans doute celle du consentement)[1305].

Ainsi, ce qui distingue un contrat de droit commun d'un contrat de traitement de données à caractère personnel est son *objet*.

354. Confirmation de cette interprétation. Plusieurs dispositions de la directive 2019/770 du 20 mai 2019 relative aux contrats de fourniture de contenus et services numériques encouragent également à retenir une telle interprétation[1306]. À l'instar du règlement européen 2016/679, cette directive distingue les situations dans lesquelles les données fournies par le consommateur sont « exclusivement traitées par

---

[1302] Monsieur Christophe Alleaume retient une distinction similaire, fondée sur l'articulation entre l'obligation principale et l'accessoire du contrat, v. C. Alleaume, « Les données à caractère personnel comme objet des contrats », *AJ Contrat* 2019, p. 373.
[1303] La CJUE considère que la nécessité est « une notion autonome du droit communautaire qui doit recevoir une interprétation de nature à répondre pleinement à l'objet » de la directive 95/46, CJUE, 16 déc. 2008, *Heinz Huber* c. *Bundesrepublik Deutschland*, C-524/06, § 52 s.
[1304] CEPD, Lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées, 8 oct. 2019, § 23 s., p. 9 s.
[1305] Pour d'autres exemples, v. CEPD, Lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées, 8 oct. 2019, § 35, p. 11 s.
[1306] Directive UE n° 2019/770 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques, *JOUE* 22 mai 2019, L-136/1, p. 1 s.

le professionnel pour fournir le contenu numérique ou le service numérique »[1307] des cas dans lesquels les données sont utilisées à d'autres fins[1308]. Il semble possible de présumer que dans ce dernier cas, la condition sur laquelle repose le traitement sera celle du consentement. Pour autant, la directive déclare s'appliquer dans les deux situations. Implicitement, le législateur reconnaît donc que lorsque le consommateur fournit des données à caractère personnel en-dehors d'une exécution contractuelle déterminé, il s'engage bien dans une relation contractuelle avec le professionnel. Cela se confirme par le domaine de la directive 2019/770 qui est relatif aux *contrats* de fourniture de contenus et services numériques.

Par ailleurs, les conclusions de l'avocat général Monsieur Maciej Szpunar confirment également que le consentement au traitement de données à caractère personnel s'inscrit souvent dans une opération contractuelle[1309]. La question préjudicielle renvoyée à la Cour de justice trouve son origine dans un litige opposant un fournisseur de services de télécommunications à une autorité de contrôle au sujet des obligations qui incombent à ce fournisseur dans le cadre de négociations contractuelles avec un client lorsqu'il s'agit de collecter et de conserver une copie de carte d'identité. Pour l'avocat général, la personne qui entend entrer dans une relation contractuelle portant sur la fourniture de services de télécommunications ne donne pas son consentement librement « dès lors qu'elle doit indiquer, par écrit, dans un contrat par ailleurs standardisé, qu'elle refuse de consentir à la collecte et à la conservation des copies de ses titres d'identité »[1310]. L'avocat général applique donc les conditions restrictives du consentement spécial au traitement de données personnelles à la conclusion d'un contrat de fourniture de services de télécommunications. La Cour de justice a suivi cette interprétation dans sa décision du 11 novembre 2020[1311].

355. Les données à caractère personnel peuvent être la contrepartie d'un contrat. Plusieurs auteurs ont remarqué que la directive 2019/2161, empreinte de

---

[1307] Art. 3 § 1 al. 2 de la directive UE nº 2019/770.
[1308] Art. 3 § 1 al. 2 de la directive UE nº 2019/770. De manière plus précise, le considérant 24 de la directive UE nº 2019/770 prévoit notamment que celle-ci « devrait également s'appliquer lorsque le consommateur donne son consentement au traitement par le professionnel, à des fins de prospection, de tout matériel constituant des données à caractère personnel, tel que des photographies ou des publications que le consommateur téléverse ».
[1309] Maciej Szpunar, concl. prés. 4 mars 2020, CJUE, *Orange România SA* c. *Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal* (ANSPDCP), C-61/19.
[1310] Maciej Szpunar, concl. prés. 4 mars 2020, CJUE, *Orange România SA* c. *Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal* (ANSPDCP), C-61/19, § 60 et 63.
[1311] CJUE, 11 nov. 2020, *Orange România SA* c. *Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal* (ANSPDCP), C-61/19, § 46 s.

pragmatisme[1312], étend l'application de la directive de 2011/83 relative aux droits des consommateurs aux contrats de fourniture de services numériques, en considérant que parce que la personne fournit ses données personnelles, ces contrats ne sont pas gratuits[1313]. Cette reconnaissance officialise ainsi « la réalité d'une "contrepartie" longtemps cachée sous le couvert d'une fausse gratuité »[1314]. Plusieurs décisions de justice avaient déjà reconnu la qualification de contrat à titre onéreux pour les contrats dont l'objet est la fourniture de données à caractère personnel. Le contrat onéreux se caractérise par le fait que chacun des cocontractants fournit quelque chose et reçoit une contrepartie voulue[1315]. Ainsi, en 2016, la cour d'appel de Paris avait rejeté la qualification de contrat à titre gratuit pour le service de réseau social proposé par Facebook et avait remarqué « que si le service proposé est gratuit pour l'utilisateur, la société Facebook Inc. retire des bénéfices importants de l'exploitation de son activité, via notamment les applications payantes, les ressources publicitaires et autres », et avait retenu « que sa qualité de professionnel ne saurait être sérieusement contestée »[1316]. Le tribunal de grande instance de Paris a également reconnu que « la fourniture de données collectées gratuitement puis exploitées et valorisées » par une entreprise « doit s'analyser en un "avantage" au sens de l'article 1107 du code civil » qui constitue la contrepartie de l'accès et de l'utilisation des services fournis par l'entreprise et qui caractérise donc la présence d'un contrat à titre onéreux[1317]. Ainsi, la contrepartie au contrat spécial peut justement être le traitement des données à caractère personnel. Il ne fait donc pas de doute que le consentement au traitement de ses données émis par la personne concernée débouche sur la formation d'un contrat spécial.

[1312] C. Zolynski, « Protection des consommateurs – Contrats de fourniture de contenus et de services numériques. À propos de la directive 2019/770/UE – Aperçu rapide », *JCP G* 2019, nº 47, p. 1181.
[1313] S. Bernheim-Desvaux, « Nouvelle donne pour les consommateurs : la directive omnibus est publiée ! », *CCC* 2020, nº 2, comm. 33.
[1314] J. Rochfeld, « Le "contrat de fourniture de contenus numériques" : la reconnaissance de l'économie spécifique "contenus contre données" », *Dalloz IP/IT* 2017, p. 15 ; J. Sénéchal, « La fourniture de données personnelles par le client *via* Internet, un objet contractuel ? », *AJ Contrats d'affaires* 2015, p. 212. Sur la qualification de l'information comme un bien, v. *supra,* nº 70.
[1315] Art. 1107 du code civil et P. Malinvaud, M. Mekki et J.-B. Seube, *Droit des obligations*, 15e éd., LexisNexis, 2019, nº 81, p. 78.
[1316] CA Paris, 2e ch., 12 févr. 2016, nº 15/08624.
[1317] TGI Paris, 7 août 2018, *UFC-Que Choisir* c. *Twitter,* nº 14/07300, p. 11 et TGI Paris, 12 févr. 2019, *UFC-Que Choisir* c. *Google,* nº 14/07224, p. 77, et TGI Paris, 9 avr. 2019, *UFC-Que Choisir* c. *Facebook*, nº 14/07928, p. 12.

356. Les conséquences de la qualification. L'opération de qualification permet de déterminer les règles applicables au contrat en sus de celles du droit commun[1318]. Selon notre proposition, dès qu'un contrat est qualifié comme un contrat de traitement de données personnelles, certaines règles particulières doivent donc lui être appliquées.

3. Règles particulières applicables au contrat spécial de traitement de données à caractère personnel

357. Plan. Plusieurs dispositions spécifiques sont applicables au contrat spécial de traitement de donnée à caractère personnel. Tout d'abord, le consentement doit revêtir certaines caractéristiques (a). Ensuite, des règles dérogatoires sont prévues en matière de capacité (b). Enfin, le retrait du consentement est régi par des dispositions particulières (c).

a. Le consentement renforcé

358. Rappel des conditions de validité du consentement en droit commun des contrats. Pour que le contrat présente les vertus qu'on s'accorde à lui prêter, encore faut-il que le consentement revête certaines qualités[1319]. Ainsi, pour être valable, le consentement doit être intègre, c'est-à-dire libre et éclairé, en d'autres termes, dépourvu de vices[1320]. L'article 1130 du code civil énumère trois vices du consentement – l'erreur, le dol et la violence – qui « 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 ». Pour être pris en considération, le vice doit donc avoir affecté le contrat de façon substantielle, c'est-à-dire qu'en l'absence de ce vice, le contrat aurait été essentiellement autre[1321].

359. La définition et les conditions de validité du consentement en droit des données à caractère personnel. En vertu de l'article 4 paragraphe 11 du règlement

---

[1318] M. Fabre-Magnan, *Droit des obligations,* t. 1, *Contrat et engagement unilatéral*, 5e éd., PUF, 2019, no 282, p. 224.
[1319] F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, no 269, p. 305.
[1320] M. Fabre-Magnan, *Droit des obligations,* t. 1, *Contrat et engagement unilatéral*, 5e éd., PUF, 2019, no 510, p. 397.
[1321] M. Fabre-Magnan, *Droit des obligations,* t. 1, *Contrat et engagement unilatéral*, 5e éd., PUF, 2019, no 511, p. 398. Certains auteurs critiquent cette interprétation et rappelle que « sans consentement, il n'est pas de contrat. L'inexistence devrait donc s'imposer. Elle reste toutefois ignorée du code, le codificateur n'en soufflant mot. Dommage ! Il faut continuer à raisonner en termes de nullité », *Rép. civ.* Dalloz, *Vo* « Contrat : formation », par N. Dissaux, 2017 (actu. 2020), no 118.

européen, le consentement est « 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 »[1322]. Ainsi, pour que le consentement soit considéré comme valable en droit des données à caractère personnel, il doit revêtir cinq critères : être une manifestation de volonté, libre, spécifique, éclairée et univoque[1323].

Le consentement du droit commun des contrats et celui du contrat spécial reposent sur des principes similaires puisque, dans les deux cas, il doit s'agir d'une manifestation de volonté libre et éclairée.

360. Analyse comparée des consentements. En dépit de cette similarité d'apparence, les critères de validité du consentement au traitement de données à caractère personnel sont plus restrictifs que ceux prévus pour le consentement en droit commun des contrats.

361. Le caractère libre. Dans le droit des données à caractère personnel, le *caractère libre* du consentement implique un réel contrôle pour les personnes concernées. Ces dernières doivent pouvoir exercer un choix sans sentir de contrainte ou subir des conséquences négatives importantes[1324]. Par exemple, la CNIL considère que le

[1322] La définition reprend celle prévue par la directive de 1995 en y apportant quelques clarifications et précisions complémentaires, v. CEPD, Guidelines 05/2020 on consent under Regulation 2016/679, 4 mai 2020, § 1 s., p. 4 s.
[1323] Pour une analyse détaillée de chacune de ces conditions, v. A. Debet, « Le consentement dans le RGPD : rôle et définition », *CCE* 2018, nº 4, dossier 9 et F. Rogue, « Capacité et consentement au traitement de données à caractère personnel et au contrat », *AJ Contrat* 2019, p. 370. Pour une analyse critique de la condition du consentement, v. E. Kosta, *Consent in the European data protection law*, Leiden Nijhoff Publishers, 2013 ; R. Brownsword, « Consent in data protection law : privacy, fair processing, and confidentiality », in *Reinventing Data Protection*, dir. S. Gutwirth, P. De Hert, S. Nouwt, Y. Poullet et C. de Terwangne, Springer, 2009, p. 83 s. ; R. Brownsword, « The cult of consent: fixation and fallacy », *Kings College Law Journal* 2004, vol. 15, nº 2, p. 223.
[1324] L'accès à un service ne peut pas, en vertu du RGPD, être soumis à la fourniture par une personne de ses données à caractère personnel (cons. 42 du règlement UE nº 2016/679 lequel prévoit que « le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice », v. aussi art. 7 § 4 du règlement UE nº 2016/679). En effet, « chaque fois que la personne est contrainte de consentir pour accéder au service, le consentement ne saurait être regardé comme libre et il est donc nécessairement douteux », N. Martial-Braz et J. Rochfeld (dir.), *Droit des données personnelles. Les spécificités du droit français au regard du RGPD,* Dalloz, 2019, nº 920, p. 155. V. La CNIL a retenu une interprétation littérale de ces textes, notamment à l'égard de Facebook, v. CNIL, décision nº 2017-075 du 27 nov. 2017, mettant en demeure la société WhatsApp et CNIL, délibération nº 2017-006 du 27 avril 2017 de la formation restreinte prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc et Facebook Ireland. À ces arguments s'ajoute également le considérant 43 du règlement UE nº 2016/679 qui affirme que le consentement ne peut être donné librement « lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement », par exemple lorsque le responsable du traitement est une autorité publique ou un employeur, v. sur ce point, CEPD, Guidelines 05/2020 on consent under Regulation 2016/679, 4 mai 2020, § 16 s., p. 8 s. Sur le caractère illusoire de la liberté de consentir, s'agissant de certains biens ou services, V. M. Fabre-Magnan, *L'institution de la liberté*, PUF, 2018, p. 13 et 76.

consentement de l'utilisateur d'un réseau social n'est pas donné librement s'il s'accompagne d'une conséquence négative importante telle que la suppression de son compte ou le fait de ne pas pouvoir utiliser l'application[1325].

Plusieurs dispositions du code civil protègent également le caractère libre du consentement. Par exemple, l'article 1140 du code civil prévoit que « il y a violence lorsqu'une partie s'engage sous la pression d'une *contrainte* qui lui inspire la crainte d'exposer sa personne, sa fortune ou celles de ses proches à un mal considérable ». Ainsi, la violence est un fondement de l'annulation du contrat lorsqu'elle est *suffisamment grave*, comme le prouve le recours à l'adjectif « considérable »[1326]. Son application est donc limitée aux cas de violence les plus graves. La réforme du droit des contrats a consacré l'élargissement de la violence à l'abus de l'état de dépendance[1327]. L'article 1143 du code civil prévoit désormais qu'il y a « violence lorsqu'une partie, abusant de l'état de dépendance dans lequel se trouve son cocontractant à son égard, obtient de lui un engagement qu'il n'aurait pas souscrit en l'absence d'une telle contrainte et en tire un avantage manifestement excessif ». Une double condition ressort de ce texte : l'état de dépendance (élément subjectif relatif à la personne) et l'abus de cet état pour en tirer un avantage *manifestement excessif* (élément objectif relatif au contenu du contrat)[1328]. Ici encore, le droit commun des contrats a des conditions d'application restrictives s'appliquant seulement aux contrats particulièrement déséquilibrés. En droit des données à caractère personnel, la condition du caractère libre du consentement protège plus largement la personne concernée.

362. Le caractère spécifique. Dans le droit des données personnelles, le caractère spécifique du consentement requiert l'obtention d'un consentement distinct et recueilli séparément pour chaque finalité poursuivie[1329]. Cela signifie qu'il ne peut pas être noyé dans des conditions générales d'utilisation ou de vente. Le consentement doit prendre la forme d'un acte de volonté séparé, au moyen par exemple d'une case à cocher pour

---

[1325] V. par ex. l'interprétation de la CNIL, décision n° 2017-075 du 27 nov. 2017, mettant en demeure la société WhatsApp.
[1326] M. Fabre-Magnan, *Droit des obligations,* t. 1, *Contrat et engagement unilatéral*, 5e éd., PUF, 2019, n° 576, p. 444.
[1327] Pour une analyse de l'état de dépendance, v. F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, n° 321, p. 359.
[1328] M. Fabre-Magnan, *Droit des obligations,* t. 1, *Contrat et engagement unilatéral*, 5e éd., PUF, 2019, n° 576, p. 444.
[1329] Cons. 32 du règlement UE n° 2016/679. V. déjà en ce sens pour les droits de la personnalité, A.-A. Hyde, *Les atteintes aux libertés individuelles par contrat. Contribution à la théorie de l'obligation,* th. Paris I, 2015, IRJS, n° 676, p. 471.

chaque finalité acceptée[1330]. C'est pourquoi, en droit des données personnelles, le consentement ne sera pas valable s'il est présenté comme une partie non négociable des conditions générales puisque la personne doit pouvoir accepter – ou refuser – chacune des finalités prévues[1331].

Il n'existe pas vraiment de disposition équivalente en droit des contrats. D'ailleurs, le droit des contrats permet les contrats d'adhésion[1332], lesquels empêchent la négociation point par point des différents éléments du contrat.

Le droit des données à caractère personnel est donc, à nouveau, plus protecteur de la personne concernée que le droit commun des contrats.

363. Le caractère éclairé. Dans le droit des données à caractère personnel, le caractère éclairé du consentement implique l'obligation de fournir certaines informations aux personnes pour les aider à consentir en toute connaissance de cause[1333]. Ainsi, pour obtenir un consentement éclairé, le responsable du traitement devra donner, en plus des lourdes exigences d'information prévues aux articles 13 et 14 du règlement européen, l'identité du responsable de traitement, la finalité, les types de données collectées, l'existence du droit de retirer son consentement, l'utilisation des données, et éventuellement, l'existence de transferts. Cette obligation vise à donner à la personne les informations nécessaires pour qu'elle comprenne les implications de son accord[1334].

En droit des contrats, deux obligations d'information précontractuelles sont prévues par le code civil[1335]. Il s'agit d'une part de l'article 1137 du code civil qui étend le dol à « la dissimulation *intentionnelle* par l'un des contractants d'une information

---

[1330] V. déjà en ce sens, CNIL, délibération nº 2017-222 du 20 juillet 2017 portant adoption d'une recommandation concernant le traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance. V. plus récemment, CNIL, délibération nº 2019-035 du 31 décembre 2013 mettant en demeure la société Électricité De France (EDF).

[1331] CEPD, Guidelines 05/2020 on consent under Regulation 2016/679, 4 mai 2020, § 13 s., p. 7 s. V. not. CE Sec., 19 juin 2020, *Société Google LLC*, nº 430810, *Lebon,* § 21 et 23.

[1332] Le contrat d'adhésion est défini par l'article 1110 du code civil comme « celui qui comporte un ensemble de clauses non négociables, déterminées à l'avance par l'une des parties ».

[1333] Cette obligation se distingue de l'obligation d'information prévue aux articles 13 et 14 du règlement UE nº 2016/679, v. A. Debet, « Le consentement dans le RGPD : rôle et définition », *CCE* 2018, nº 4, dossier 9. La CNIL et le Conseil d'État retiennent une interprétation stricte de cette condition, v. CNIL, délibération nº 2019-001 du 21 janvier 2019 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google LLC, spéc. nºs 141 s. et sa confirmation par la décision CE Sec., 19 juin 2020, nº 430810, *Société Google LLC*, *Lebon*, § 21.

[1334] Parmi la liste d'informations figurent notamment l'identité du responsable du traitement, la finalité du traitement, les données collectées et leur utilisation, le droit de retirer son consentement, v. CEPD, Guidelines 05/2020 on consent under Regulation 2016/679, 4 mai 2020, § 64, p. 15 s.

[1335] Sur le formalisme informatif et la protection individuelle du consommateur, v. J. Rochfeld, « Du statut du droit contractuel "de protection de la partie faible" : les interférences du droit des contrats, du droit du marché et des droits de l'homme », in *Mélanges G. Viney*, LGDJ, 2008, p. 835 s., nºs 19 s., spéc. p. 857 s.

dont il sait le caractère déterminant par l'autre partie », et d'autre part de l'article 1112-1 qui reconnaît un devoir général d'information imposé pendant la période des négociations[1336]. Ce devoir général d'information se limite aux informations ayant une *importance déterminante*, c'est-à-dire aux informations qui, si elles avaient été connues par le cocontractant, l'auraient découragé de conclure le contrat ou l'auraient conduit à le conclure à des conditions substantiellement différentes[1337].

Ici encore, le droit des données à caractère personnel est plus précis sur les modalités d'obtention du consentement, et la protection de celui-ci semble donc plus effective. Un élément supplémentaire doit également être pris en considération au moment d'établir si le consentement est donné de manière éclairée. Il s'agit du moment auquel le consentement est demandé. En effet, celui-ci a un impact considérable sur son caractère éclairé. Les organismes devraient donc faire leurs demandes d'accès aux données lorsque les utilisateurs souhaitent utiliser la fonctionnalité en question (par exemple, demander l'accès au répertoire de contact pour passer un appel), et non pas lors de l'inscription[1338].

364. Le caractère univoque. Dans le droit des données à caractère personnel, le caractère univoque du consentement est plus strict que celui résultant du droit commun des contrats. En effet, le principe en droit des contrats est que le silence ne vaut pas acceptation[1339]. La volonté doit donc être extériorisée, ce qui peut se faire par écrit, par oral ou par un geste[1340]. Le droit des contrats reconnaît toutefois, dans quelques cas limités, une valeur juridique au silence[1341].

Au contraire, le droit des données à caractère personnel ne connaît pas d'exception, le silence n'est donc jamais considéré comme le signe d'une acceptation[1342]. En effet, selon le CEPD, « le recours à des cases cochées par défaut

---

[1336] M. Fabre-Magnan, *Droit des obligations,* t. 1, *Contrat et engagement unilatéral*, 5e éd., PUF, 2019, no 556, p. 429.
[1337] Art. 1112-1 al. 3 du code civil, lequel prévoit qu'ont « une importance déterminante les informations qui ont un lien direct et nécessaire avec le contenu du contrat ou la qualité des parties ».
[1338] G29, WP 260 rév. 01, Lignes directrices sur la transparence au sens du règlement 2016/679, 11 avr. 2018, p. 24.
[1339] Sur la question du silence en droit des contrats, v. N. Martial-Braz, « L'ambivalence du silence en droit des contrats », in *Le silence saisi par le droit privé,* dir. N. Martial-Braz et F. Terryn, IRJS, 2014, p. 9 s., spéc. p. 11 s.
[1340] Le considérant 32 du règlement UE no 2016/679 prévoit que l'acte positif clair peut être effectué notamment « au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale ».
[1341] Notamment lorsque la loi le prévoit, les usages et les relations d'affaires ou encore les circonstances particulières, v. M. Fabre-Magnan, *Droit des obligations,* t. 1, *Contrat et engagement unilatéral*, 5e éd., PUF, 2019, nos 439 s., p. 343 s.
[1342] F. Rogue, « Capacité et consentement au traitement de données à caractère personnel et au contrat », *AJ Contrat* 2019, p. 370. La CJUE, reprenant l'interprétation de son avocat général, a précisé que « l'exigence d'une "manifestation" de volonté de la personne concernée évoque clairement un comportement actif et non pas

n'est pas valable en vertu du RGPD. Le silence ou l'inactivité de la personne concernée, ainsi que le simple fait qu'elle continue à utiliser un service, ne peuvent être considérés comme une indication active de choix »[1343]. La CNIL a d'ailleurs récemment confirmé une telle interprétation, notamment à l'égard des cookies et des traceurs[1344]. Malgré ces principes protecteurs, le CEPD reconnaît une vraie lassitude des personnes face aux sollicitations répétées des services numériques[1345]. D'ailleurs, comme le remarquait de manière imagée Monsieur Emmanuel Netter, « en ligne plus encore qu'ailleurs, l'utilisateur a tendance à foncer comme un taureau furieux vers l'instant où il pourra bénéficier du service »[1346]. Ces éléments font relativiser les différences existantes sur le caractère univoque du consentement entre le doit des contrats et le droit des données à caractère personnel.

365. Les conditions du consentement du contrat spécial sont plus protectrices des personnes. Pour résumer, les caractères du consentement en droit des données à caractère personnel et en droit des contrats sont fondés sur des principes similaires. Toutefois, les conditions de validité du consentement sont relativement plus strictes en droit des données à caractère personnel[1347]. Elles ont pour objectif d'aider les personnes

---

passif. Or, un consentement donné au moyen d'une case cochée par défaut n'implique pas un comportement actif de la part de l'utilisateur d'un site Internet », CJUE, 1 oct. 2019, *Bundesverband* c. *Planet49,* C-673/17, § 52 s. ; plus récemment, v. Maciej Szpunar, concl. prés. 4 mars 2020, CJUE, *Orange România SA* c. *Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal* (ANSPDCP), C-61/19, § 44 s. V. aussi CE Sec. 19 juin 2020, n° 430810, *Société Google LLC*, § 21, *Lebon*. Comp. avec le consentement de la personne à l'exploitation de droits de la personnalité, v. *Rép. civ.* Dalloz, *V°* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), n° 199. La Cour de cassation a ainsi admis que « le consentement à la diffusion d'images de la personne ou de faits de sa vie privée peut être tacite », v. Cass. civ. 1re, 7 mars 2006, n° 04-20.715, *Bull. civ.* 2006, I, n° 139, p. 128 ; Cass. civ. 1re, 13 nov. 2008, n° 06-16.278, *Bull. civ.* 2008, I, n° 259. Toutefois, la Cour de cassation interprète le consentement de façon restrictive, v. Cass. civ. 1re, 4 nov. 2011, n° 10-24.761, *Bull. civ.* 2011, I, n° 196.

[1343] CEPD, Guidelines 05/2020 on consent under Regulation 2016/679, 4 mai 2020, § 77, p. 18.

[1344] CNIL, délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019, § 26 s. La délibération de juillet 2019 avait été partiellement retoquée par le Conseil d'État, CE Sec., 19 juin 2020, n° 434684, *Association des agences-conseils en communication et autres*, § 10, *Lebon T.* Le Conseil d'État avait considéré que l'édiction d'une interdiction générale et absolue dans une délibération, instrument de droit souple, excédait les pouvoirs dont disposait la CNIL. Il reprenait la définition qu'il avait donnée du droit souple dans son étude de 2013, lequel est considéré comme « l'ensemble des instruments réunissant trois conditions cumulatives : ils ont pour objet de modifier ou d'orienter les comportements de leurs destinataires en suscitant, dans la mesure du possible, leur adhésion ; ils *ne créent pas par eux-mêmes de droits ou d'obligations pour leurs destinataires* ; ils présentent, par leur contenu et leur mode d'élaboration, un degré de formalisation et de structuration qui les apparente aux règles de droit », v. Conseil d'État, « Le droit souple », *Rapport Public 2013*, La Documentation française, 2013, p. 61.

[1345] CEPD, Guidelines 05/2020 on consent under Regulation 2016/679, 4 mai 2020, § 97, p. 19.

[1346] E. Netter, « Sanction à 50 millions d'euros : au-delà de Google, la CNIL s'attaque aux politiques de confidentialité obscures et aux consentements creux », *Dalloz IP/IT* 2019, p. 165.

[1347] Le consentement en matière de donnée à caractère personnel ne pourra pas être considéré comme valable dans des situations de déséquilibre entre les parties. En effet, le considérant 43 du règlement UE n° 2016/679 prévoit que celui-ci ne constitue pas un fondement juridique valable « lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une

concernées à faire un choix informé en leur permettant d'exercer un véritable contrôle sur leurs données. Cet encadrement est *de facto* moins nécessaire lorsque le fondement du traitement est le contrat. L'obligation contractuelle intervient alors comme une barrière encadrant les traitements de données : seules les données strictement nécessaires à l'exécution du contrat peuvent être licitement traitées[1348]. Dès lors que le traitement est fondé sur le consentement, le responsable du traitement devrait mettre en œuvre ces conditions strictes. En plus d'un consentement renforcé, le responsable du traitement est également soumis à certaines règles particulières en matière de capacité.

b. La capacité à contracter

366. Rappel des règles relatives à la capacité en droit commun des contrats. L'article 1145 du code civil pose un principe de capacité des personnes physiques. L'exception et ses contours sont détaillés dans l'article suivant, lequel prévoit que « sont incapables de contracter dans la mesure définie par la loi : 1° les mineurs non émancipés ; 2° les majeurs protégés au sens de l'article 425 ». Ainsi, les mineurs non émancipés sont frappés d'une incapacité d'exercice[1349], c'est-à-dire qu'ils ne peuvent contracter que par l'intermédiaire de leur représentant, administrateur légal ou tuteur[1350]. Deux articles viennent toutefois réduire la portée de cette règle. D'une part, l'article 388-1-1 du code civil établit que « l'administrateur légal représente le mineur dans tous les actes de la vie civile, sauf les cas dans lesquels la loi ou l'usage autorise les mineurs à agir eux-mêmes ». D'autre part, l'article 1148 du code civil reconnaît aux individus incapables de contracter la possibilité d'accomplir seuls les « actes courants autorisés par la loi ou l'usage, pourvu qu'ils soient conclus à des conditions normales »[1351]. Pour le dire plus simplement, le mineur ne peut pas contracter seul, sauf lorsque la loi ou l'usage l'y autorise[1352].

---

autorité publique ». Les lignes directrices du CEPD ajoutent également qu'un tel déséquilibre peut se retrouver dans le cadre des relations de travail, vue la dépendance résultant de la relation employeur et employé, v. CEPD, Guidelines 05/2020 on consent under Regulation 2016/679, 4 mai 2020, § 21 s., p. 9 s.

[1348] D'ailleurs, le CEPD précise que la locution « nécessaire à l'exécution d'un contrat » doit être interprétée de façon restrictive, v. CEPD, Guidelines 05/2020 on consent under Regulation 2016/679, 4 mai 2020, § 30 s., p. 10 s.

[1349] G. Loiseau, *Le droit des personnes*, 2e éd., Ellipses, 2020, n° 50, p. 42.

[1350] F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, n° 152, p. 187.

[1351] V. déjà en ce sens Cass. civ. 1re, 9 mai 1972, n° 71-10.361, *Bull. civ.* I, n° 122, p. 110.

[1352] L'articulation entre ces deux exceptions a fait l'objet de critiques de la part de la doctrine, v. not. F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, n° 152, p. 187 s. ; v. aussi, M. Latina et G. Chantepie, *Le nouveau droit des obligations*, 2e éd., Dalloz, 2018, nos 358 s., p. 309 s.

367. Les règles relatives au consentement des enfants en droit des données personnelles. Le règlement européen prévoit, pour la première fois dans cette matière, un dispositif spécifique pour les personnes les plus jeunes[1353]. Le texte fait de multiples références à la notion d'« enfant », sans pour autant prendre le soin de la définir[1354]. Sans aucun doute, cette notion doit être rapprochée de celle de « mineur »[1355], puisque l'article 8 du règlement européen prévoit plusieurs seuils d'âge, tous en dessous de 18 ans.

Dans le considérant 38 de ce texte, le législateur européen pose un principe de protection renforcée pour les enfants « 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 »[1356]. La mise en œuvre de cette « protection » érigée par le règlement européen est relativement surprenante puisqu'il aménage un régime dérogatoire au principe d'incapacité des mineurs. En effet, l'article 8 du règlement européen consacre « un nouvel îlot de capacité naturelle »[1357], permettant à certains mineurs de consentir valablement au traitement de leurs données personnelles lorsque ce traitement est lié à une offre directe de service de la société de l'information[1358]. Le mineur peut donc agir seul lorsque plusieurs conditions sont réunies. Tout d'abord, il faut que le responsable du traitement traite les données sur le fondement du consentement. Ensuite, le mineur doit avoir un âge déterminé par la loi. En France, cet âge est fixé à 15 ans, mais dans les autres États membres, il varie entre 13 et 16 ans[1359]. Par exemple, en Angleterre ou en Belgique, il est fixé à 13 ans, alors

---

[1353] Si la loi du 6 janvier 1978 ne comportait aucune disposition spécifique pour les mineurs, la doctrine de la CNIL faisait appel au droit commun et requérait en principe le consentement des parents pour la collecte de données personnelles des mineurs, v. CNIL, « Internet et la collecte de données personnelles auprès des mineurs », juin 2001, p. 15 s.

[1354] Le législateur européen s'est sans doute inspiré de la recommandation de l'OCDE dans ce domaine, OCDE, « Recommandation du Conseil sur la protection des enfants sur Internet », 2012 ; ou de la notion de *child* prévue par la législation fédérale américaine *Children's Online Privacy Protection Act*. Sur les similarités avec cette loi, v. *infra*, nº 368. Il convient de noter que tous les pays de l'Union européenne placent la majorité civile à l'âge de 18 ans.

[1355] Le mineur est classiquement défini comme l'« individu qui n'a pas atteint l'âge de la majorité », G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vº* « Mineur », sens 1.

[1356] Pourtant, plusieurs études ont montré que, contrairement à une opinion répandue, les personnes plus jeunes avaient souvent une meilleure connaissance des paramètres de confidentialité et des façons de protéger leur vie privée en ligne que les adultes, v. C. Hoofnagle, J. King, S. Li et J. Turow, « How different are young adults from older adults when it comes to information privacy attitudes and policies ? », 14 avr. 2010 ; Pew Research Center, « The state of privacy in post-Snowden America », *FactTank* 21 sept. 2016 ; National Cyber Security Alliance, « Keeping Up with Generation App », 2017.

[1357] T. Douville, « La protection des données à caractère personnel des mineurs et des majeurs protégés », *RLDC* 2018, nº 162, p. 42.

[1358] F. Rogue, « Capacité et consentement au traitement de données à caractère personnel et au contrat », *AJ Contrat* 2019, p. 370.

[1359] Le règlement européen fixe l'âge à seize ans, mais les États peuvent abaisser ce seuil jusqu'à treize ans. La France a choisi un seuil d'âge de quinze ans, v. art. 45 de la loi nº 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018. Pour un tableau synthétique sur l'âge du consentement du mineur en

qu'en Allemagne ou au Luxembourg, il est fixé à 16 ans[1360]. Le responsable du traitement est chargé d'une obligation de moyens exigeante puisqu'il doit mettre en œuvre tous les moyens raisonnables pour s'assurer de l'âge de la personne et éventuellement obtenir le consentement de ses représentants légaux[1361]. Enfin, deux conditions relatives au service doivent être vérifiées. D'une part, il doit s'agir d'une offre de service de la société de l'information, c'est-à-dire d'un service fourni à distance, par voie électronique et à la demande individuelle d'un destinataire de service[1362]. En pratique, il s'agit notamment des réseaux sociaux, des moteurs de recherche ou des jeux en ligne[1363]. D'autre part, le service doit être destiné aux enfants, c'est-à-dire que l'obligation ne concerne pas l'offre de service qui indiquerait clairement s'adresser aux personnes âgées de plus de dix-huit ans, tant que cela n'est pas contredit par le reste de l'activité (notamment par le contenu du site ou des campagnes de publicité)[1364]. Lorsque les règles relatives au consentement des enfants s'appliquent, le responsable du traitement doit adapter la terminologie utilisée dans son information et sa communication, afin que les documents soient rédigés « en des termes clairs et simples que l'enfant peut aisément comprendre »[1365].

En dehors de cette situation particulière dans laquelle le mineur peut consentir seul au traitement de ses données, les titulaires de l'autorité parentale doivent consentir avec lui et ce, quel que soit son âge[1366].

Il est possible de se demander si les exceptions prévues par le droit commun des contrats, notamment celles liées à l'usage, peuvent s'ajouter à cet îlot de capacité. Pour Monsieur Thibault Douville, il n'y a pas de réponse catégorique : « tout dépend certainement de la nature des données traitées, des finalités poursuivies par le responsable du traitement et des risques créés pour le mineur »[1367]. Ainsi, l'exception autorisant un mineur à consentir seul au traitement de ses données pourrait être enrichie

---

fonction des États, v. O. Tambou, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, nº 149, p. 141.

[1360] I. Milkaite et E. Lievens, « *Status quo* regarding the child's article 8 GDPR age of consent for data processing across the EU », *Better Internet for Kids* 20 déc. 2019.

[1361] CEPD, Guidelines 05/2020 on consent under Regulation 2016/679, 4 mai 2020, § 131 s., p. 27 s.

[1362] L'article 4 du règlement UE nº 2016/679 renvoie à la définition fournie par la directive UE nº 2015/1535 du Parlement européen et du Conseil prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, *JOUE* 17 sept. 2015, L-241, p. 1 s.

[1363] Le règlement européen semble donc encourager une interprétation large des contrats dont l'objet est le traitement de données à caractère personnel.

[1364] CEPD, Guidelines 05/2020 on consent under Regulation 2016/679, 4 mai 2020, § 130, p. 27.

[1365] Cons. 58 du règlement UE nº 2016/679.

[1366] T. Douville, « La protection des données à caractère personnel des mineurs et des majeurs protégés », *RLDC* 2018, nº 162, p. 42.

[1367] T. Douville, « La protection des données à caractère personnel des mineurs et des majeurs protégés », *RLDC* 2018, nº 162, p. 42.

d'autres cas dans lesquels l'usage admettrait que le mineur contracte seul. Le régime instauré par le règlement européen pour le consentement des mineurs se rapproche fortement de celui mis en place par la loi fédérale américaine COPPA.

368. Rapprochements avec la loi américaine COPPA. La loi fédérale américaine *Children's Online Privacy Protection Act* (COPPA) adoptée en 1998[1368] vise à protéger la *privacy* en ligne des enfants de moins de treize ans et à encourager les parents à s'impliquer dans leurs activités en ligne. Cette loi interdit aux exploitants de site ou de services en ligne destinés aux enfants[1369] de collecter, d'utiliser ou de diffuser des informations personnelles d'un enfant de moins de 13 ans sans le consentement d'un de ses représentants légaux[1370]. Modifié en janvier 2013[1371], le nouveau régime élargit les acteurs et les activités couvertes, notamment en soumettant aux règles les tiers collectant des informations *via* des opérateurs web. Il étend également la définition d'information personnelle[1372], redéfinit les exceptions existantes, précise les méthodes pour obtenir un consentement parental, renforce l'information préalable des parents et consolide les pouvoirs de la FTC sur les programmes de protection[1373].

Les auteurs s'accordent pour dire que COPPA est loin d'être un instrument parfait pour garantir efficacement la protection des données des mineurs en ligne. L'une des critiques récurrentes est liée au seuil d'âge, qui aurait tendance à faire mentir les enfants sur celui-ci[1374]. Cette critique est d'autant plus appropriée que les technologies pour s'assurer de l'âge d'une personne, au risque d'être trop intrusives, ne permettent pas de garantir la véracité de l'âge déclaré[1375].

[1368] Pub. L. du 21 avr. 2000, nº 105-277, codifiée au 15 U.S.C. § 6501 s.
[1369] L'article 15 U.S.C. § 6501 (2) définit les *operator* assez largement puisqu'il s'agit de « toute personne qui opère un site Internet ou un service en ligne et qui collecte ou traite les données personnelles de ses visiteurs ».
[1370] 15 U.S.C. § 6502.
[1371] T. Gadbwa, « Legislative update : Children's Online Privacy Protection Act of 1998 », *Children's Legal Rights Journal* 2016, vol. 36, p. 228 s. [36 CHILD. LEGAL. RTS. J. 228], spéc. p. 64 ; v. aussi FTC, « Children's Online Privacy Protection rule », 16 C.F.R. 312, Fed. Reg., vol. 78, nº 12, 17 janv. 2013.
[1372] La notion d'information personnelle inclut désormais : un prénom et un nom ; une adresse postale ; des informations de contact ; un pseudonyme ou un nom d'utilisateur : un numéro de téléphone ; un numéro de sécurité sociale ; un identifiant qui permet de suivre l'utilisateur, notamment un cookie, une adresse IP ou un numéro unique d'identification d'un appareil ; l'image et la voix d'une personne matérialisée ; des informations de localisation qui permettent d'identifier un nom de rue ou de ville ; ou des informations concernant l'enfant ou les parents recueillies en ligne et liées à un identifiant, 16 C.F.R. § 312.
[1373] D. Hostetler et S. Okada, « Virtual solutions of the amended Children's Online Privacy Protection Act (COPPA) rule », *North Carolina Journal of Law & Technology Online* 2013, vol. 14, p. 167 s. [14 N.C.J.L. & TECH. ON. 167], spéc. p. 184. Pour les définitions, v. 15 U.S.C. § 6501.
[1374] L. Matecki, « Update : COPPA is ineffective legislation ! Next steps for protecting youth privacy rights in the social networking era », *Northwestern Journal of Law & Social Policy* 2010, vol. 5, p. 369 s. [5 NW. J. L. & SOC. POL'Y 369], spéc. p. 370.
[1375] FTC, « Implementing the Children's Online Privacy Protection Act : a report to Congress », févr. 2007, p. 29.

Cette critique est parfaitement transposable au système européen[1376]. Malgré ces difficultés, les législateurs ont tendance à étendre ce type d'obligations de vérification d'âge à d'autres matières[1377].

En plus de ces dispositions spéciales en lien avec le consentement et la capacité, le règlement européen a également offert la possibilité aux personnes concernées de retirer leur consentement.

c. Le retrait du consentement

369. Rappel des règles de retrait du consentement en droit des contrats. Longtemps, le contrat a été considéré comme « un temple de la bilatéralité au sein duquel la volonté unilatérale des parties n'a plus sa place », empêchant ainsi les contractants de se dégager unilatéralement du lien contractuel les unissant[1378]. Le droit des contrats a évolué pour s'adapter aux besoins de la société, notamment au développement des contrats de longue durée, et a aménagé des dérogations à ce principe. Les facultés de rétractation, expressément autorisées par l'article 1122 du code civil, de résiliation unilatérale, voire de modification ont trouvé une place grandissante dans cette matière[1379]. Ainsi, les contrats à durée indéterminée impliquent un pouvoir de résiliation unilatérale[1380], règle qui s'inscrit dans la prohibition des engagements perpétuels et la sauvegarde de la liberté de la personne.

370. Le retrait du consentement dans les contrats portant sur des droits de la personnalité. La doctrine est divisée sur la possibilité de révoquer unilatéralement les conventions portant sur les droits de la personnalité. Certains auteurs considèrent que « le consentement de la partie intéressée est révocable jusqu'à l'exécution et même parfois au-delà de l'exécution de la convention »[1381]. Selon ces auteurs, la particularité

[1376] Elles ont d'ailleurs été formulées par la doctrine, v. B. Charrier, « Le consentement exprimé par les mineurs en ligne », *Dalloz IP/IT* 2018, p. 333.
[1377] V. par ex. l'adoption récente d'une obligation pour les personnes « dont l'activité est d'éditer un service de communication au public en ligne » de vérifier la majorité des personnes souhaitant avoir accès à un contenu pornographique, art. 23 de la loi n° 2020-936 du 30 juill. 2020 visant à protéger les victimes de violences conjugales, *JORF* 31 juill. 2020, n° 0187, texte 2.
[1378] G. Chantepie et M. Latina, *La réforme du droit des obligations*, 2e éd., Dalloz, 2018, n° 517, p. 436.
[1379] G. Chantepie et M. Latina, *La réforme du droit des obligations*, 2e éd., Dalloz, 2018, n° 517, p. 436 s.
[1380] O. Porumb, *La rupture des contrats à durée indéterminée par volonté unilatérale,* th. Paris, 1937, p. 8 ; B. Houin, *La rupture unilatérale des contrats synallagmatiques,* th. Paris II, 1973, p. 27 s. et p. 113 ; I. Pétel-Teyssié, *Les durées d'efficacité du contrat*, th. Montpellier, 1984, n° 333, p. 355 ; F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, n° 660, p. 733. Ce principe est désormais formulé dans l'article 1211 du code civil.
[1381] V. not. R. Nerson, *Les droits extrapatrimoniaux*, th. Lyon, 1939, n° 191, p. 423 s. ; J. Stoufflet, « Le droit de la personne sur son image », *JCP* 1957, I, p. 1374, n° 33 ; J. Ravanas, *La protection des personnes contre la*

de ces conventions aurait pour effet d'octroyer au titulaire du droit de la personnalité une prérogative unilatérale de révocation[1382]. Cette conception est largement critiquée par d'autres auteurs qui affirment qu'une telle prérogative viderait l'accord de toute utilité, dans la mesure où celui-ci vise précisément à mettre à l'abri le co-contractant contre une action en contestation du titulaire du droit de la personnalité cédé[1383]. Une telle interprétation, reconnue par la Cour de cassation[1384], paraît justifiée pour les contrats portant sur certains droits de la personnalité, notamment pour l'emploi du nom à titre de marque, de dénomination sociale ou de nom commercial, dès lors que ces contrats requièrent une sécurité juridique avec laquelle le retrait unilatéral du consentement du titulaire n'est pas compatible. Reconnaître un tel pouvoir unilatéral remettrait en cause l'équilibre du contrat[1385], voire le priverait de son utilité[1386]. Pour autant, de telles conséquences sont difficilement transposables pour les contrats de traitement de données personnelles, notamment parce que beaucoup d'entre eux sont des contrats d'adhésion et qu'ils n'ont pas le caractère *intuitu personae* que l'on retrouve dans les contrats traditionnels portant sur d'autres droits de la personnalité[1387].

371. Le retrait du consentement en matière de données à caractère personnel. Le droit des données personnelles a consacré, sans trop de difficulté, la possibilité pour la personne concernée de retirer son consentement à tout moment, et sans que ce retrait n'ait d'effet sur elle[1388]. Cet effacement doit être considéré comme une manifestation unilatérale et libre de volonté qui fait perdre à un tiers un droit (celui de traiter les données personnelles) dont il disposait jusqu'alors[1389]. Un tel pouvoir conduit Madame

---

réalisation et la publication de leur image, th. Aix-en-Provence, 1978, LGDJ, nº 288, p. 306 s. V. déjà au sujet des contrats relatifs à la personne physique et la capacité de retirer le consentement, « jusqu'au dernier moment », A. Jack, « Les conventions relatives à la personne physique », *Revue critique de législation et de jurisprudence* 1933, p. 362 s., spéc. p. 385 s.

[1382] J. Stoufflet, « Le droit de la personne sur son image », *JCP* 1957, I, p. 1374, nº 33 ; J. Ravanas, *La protection des personnes contre la réalisation et la publication de leur image,* th. Aix-en-Provence, 1978, LGDJ, nº 288, p. 306 ; G. Goubeaux, *Traité de droit civil. Les personnes*, LGDJ, 1989, nº 323, p. 302 ; A.-M. Luciani, *Les droits de la personnalité. Du droit interne au droit international privé*, th. Paris I, 1996, nº 78, p. 75 s. ; B. Teyssié, *Droit des personnes*, 21e éd., LexisNexis, 2019, nº 262, p. 236.

[1383] G. Loiseau, *Le nom, objet d'un contrat*, th. Paris I, 1995, LGDJ, nº 319, p. 309 ; G. Loiseau, « Le droit à l'image aux prises avec la force obligatoire des conventions », *Dr et pat.* 2004, nº 127, p. 96. V. déjà, R. Nerson, *Les droits extrapatrimoniaux*, th. Lyon, 1939, nº 185, p. 403 s.

[1384] Cass. civ. 1re, 10 mars 2004, nº 02-16.354, *Bull. civ.* 2004, II, nº 118, p. 99.

[1385] I. Pétel-Teyssié, *Les durées d'efficacité du contrat*, th. Montpellier, 1984, nº 336, p. 363.

[1386] G. Loiseau, *Le nom, objet d'un contrat*, th. Paris I, 1995, LGDJ, nº 323, p. 315.

[1387] Le litige à l'origine de la décision de la Cour de cassation était lié au retrait de l'accord donné par une personne à la réalisation d'un reportage, au cours duquel elle avait accepté d'être filmée et que ses propos soient enregistrés. La Cour de cassation considérait que le retrait du consentement, en l'absence de justification réelle d'un manquement à la finalité visée dans l'autorisation qu'elle avait donnée, n'était pas légitime, v. Cass. civ. 1re, 10 mars 2004, nº 02-16.354, *Bull. civ.* 2004, II, nº 118, p. 99.

[1388] S. Pellet, « RGPD : l'effacement du consentement », *RGDA* 2019, nº 1, p. 6.

[1389] S. Pellet, « RGPD : l'effacement du consentement », *RGDA* 2019, nº 1, p. 6.

Sophie Pellet à affirmer que « aucun contrat ne peut naître entre le responsable du traitement et la personne physique dont l'objet serait le traitement des données »[1390]. Pourtant, plusieurs éléments remettent largement en doute une telle interprétation. Ainsi, par exemple, le considérant 39 de la directive 2019/770 affirme que le droit de retirer son consentement pour le traitement de données à caractère personnel devrait « s'appliquer pleinement en lien avec tout contrat relevant de la présente directive »[1391]. Le retrait du consentement au contrat spécial de traitement de données à caractère personnel est donc expressément reconnu pour les contrats visés par cette directive, ce qui confirme qu'il n'empêche pas la reconnaissance de l'existence d'un contrat. Par ailleurs, de tels retraits de consentement sont reconnus dans d'autres domaines.

372. Le retrait du consentement dans certains contrats. La possibilité pour la personne de retirer son consentement d'un contrat est une figure connue de plusieurs domaines du droit dans lesquels des contrats existent. Par exemple, le droit des assurances connaît de nombreux cas de résiliation issus de la volonté unilatérale de l'une des parties[1392]. Parfois, l'insertion dans le contrat d'une clause de résiliation est même imposée par la loi[1393]. Le droit médical prévoit également des aménagements au principe d'interdiction du droit commun des contrats[1394]. Par exemple, l'article L. 1111-4 du code de la santé publique établit 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 ». Comme le remarque Monsieur Benjamin Moron-Puech, plusieurs raisons permettent d'affirmer qu'une telle capacité de rétractation du patient ne déroge nullement au principe de force obligatoire du contrat établi à l'article 1103 du code civil[1395]. Tout d'abord, cet article n'implique pas que les conventions ne peuvent pas être révoquées, même unilatéralement[1396]. Ensuite, l'article 1193 du code civil prévoit la révocation de la convention dans deux

---

[1390] S. Pellet, « RGPD : l'effacement du consentement », *RGDA* 2019, n° 1, p. 6.
[1391] Conformément au renvoi opéré par la directive UE n° 2019/770, l'article 7 § 3 du règlement UE n° 2016/679 prévoit qu'une fois le consentement retiré, le traitement ultérieur de données n'est plus licite.
[1392] *Rép. civ.* Dalloz, *V°* « Assurance de personnes : vie – prévoyance », par J. Kullmann, 2013 (actu. 2020), n^os^ 396 s. V. par ex. l'article L. 113-12 du code des assurances qui ouvre plusieurs facultés de résiliation unilatérale.
[1393] *Rép. civ.* Dalloz, *V°* « Résolution – résiliation », par C. Chabas, oct. 2010 (actu. 2018), n° 287.
[1394] V. not. l'analyse de la notion de consentement en droit médical, M. Le Goues, *Le consentement du patient en droit de la santé*, th. Perpignan, 2015, p. 446 s.
[1395] B. Moron-Puech, *Contrat ou acte juridique ? Étude à partir de la relation médicale*, th. Paris II, 2016, LGDJ, n° 131, p. 101.
[1396] B. Moron-Puech, *Contrat ou acte juridique ? Étude à partir de la relation médicale*, th. Paris II, 2016, LGDJ, n° 131, p. 101.

hypothèses, une spéciale (le consentement mutuel) et une générale (les causes que la loi autorise). Or, et comme le relève le même auteur, « parmi les causes que la loi pourrait autoriser, il y a justement la révocation du contrat par l'une des parties »[1397].

Il existe plusieurs domaines dans lesquels la loi autorise l'une des parties à retirer son consentement, et donc à anéantir unilatéralement le contrat. Ainsi, rien n'empêche de considérer qu'un contrat est valablement formé, même si la personne concernée peut, *a posteriori*, retirer son consentement au traitement de ses données.

373. Les limites au retrait du consentement en droit des données personnelles. La limite principale au retrait du consentement réside dans son absence de rétroactivité puisque le paragraphe 3 de l'article 7 du règlement européen prévoit que « le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait ». Cette absence de rétroactivité trouve elle-même une limite puisque la personne concernée a toujours la possibilité de demander l'effacement de ses données[1398]. Parfois, la combinaison de ces deux prérogatives peut avoir de lourdes conséquences pour les responsables du traitement.

374. La reconnaissance d'une limite à l'effacement des données. Certains modèles d'apprentissage automatique utilisent des réseaux neuronaux entraînés par des données personnelles[1399]. En pratique, il pourrait être particulièrement complexe (et onéreux) pour le responsable du traitement de supprimer les données ayant enrichi un tel modèle, et des difficultés techniques pourraient surgir en cas de suppression. D'une part, l'identification des données personnelles à supprimer, au sein de l'ensemble de données ayant entraîné les réseaux de neurones, peut se révéler complexe[1400]. D'autre part, imposer la suppression de ces données ne serait pas sans conséquence pour le modèle qui devrait être entraîné à nouveau sans les données. Cela pourrait avoir un coût extrêmement élevé pour le responsable du traitement.

Pour éviter de telles conséquences qui semblent disproportionnées, certaines limites à l'exercice de ces prérogatives pourraient être instaurées. Ainsi, et sur le

---

[1397] B. Moron-Puech, *Contrat ou acte juridique ? Étude à partir de la relation médicale*, th. Paris II, 2016, LGDJ, nº 131, p. 102.
[1398] Art. 17 du règlement UE nº 2016/679.
[1399] Pour une étude sur l'intelligence artificielle, v. C. Villani (dir.), « Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne », 28 mars 2018.
[1400] Sans doute les données les plus exceptionnelles, c'est-à-dire celles qui ont le plus faible nombre d'occurrence, risquent d'être plus aisées à retrouver au sein d'un tel modèle.

modèle de l'article 1221 du code civil relatif à l'exécution forcée déraisonnable, il serait possible d'envisager que ces droits soient encadrés lorsque le coût de leur mise en œuvre s'avèrerait manifestement disproportionné par rapport à l'intérêt de la personne concernée[1401]. D'ailleurs, le paragraphe 3 de l'article 16 de la directive 2019/770 prévoit justement une solution similaire pour le contenu autre que les données à caractère personnel en cas de résolution. Le professionnel a le droit de continuer à utiliser ce contenu, même après le retrait du consentement, s'il a « été agrégé avec d'autres données par le professionnel et ne peut être désagrégé, ou ne peut l'être que moyennant des efforts disproportionnés ». Une transposition de cette disposition au consentement au traitement de données à caractère personnel semble parfaitement envisageable et justifiée. Bien sûr, en tant que reflet de la personne, la donnée à caractère personnel ne doit pas être assimilée à un simple contenu. Toutefois, il semble que dans la plupart des situations, l'intérêt du responsable du traitement pour ces traitements particuliers dépasse celui de l'individu sur ses données.

La reconnaissance de l'existence d'un contrat spécial entraîne plusieurs conséquences.

4. Les conséquences de la reconnaissance du contrat spécial de traitement de données à caractère personnel

375. Le contrat spécial de traitement de données à caractère personnel. Selon notre analyse, il est possible de considérer que le règlement européen a instauré un nouveau contrat spécial. L'ensemble des conditions nécessaires à la création d'un tel contrat sont réunies puisque la volonté du responsable du traitement rencontre celle de la personne concernée dans le but de produire des effets de droit. Ce contrat a pour objet principal le traitement de données personnelles. Il prévoit des dispositions particulières qui dérogent au droit commun des contrats en ce qui concerne la formation du contrat (consentement renforcé et certaines règles de capacité) et son exécution (retrait du consentement de la personne concernée).

376. Les conséquences de la reconnaissance d'un tel contrat spécial. Il est fréquent de lire que la contractualisation des éléments de la personnalité a conduit à

[1401] M. Latina et G. Chantepie, *Le nouveau droit des obligations,* 2e éd., Dalloz, 2018, no 633, p. 582.

une monétisation de la personne[1402]. Les dispositions particulières applicables au contrat spécial portant sur le traitement de données personnelles semblent atténuer cette affirmation. Au contraire même, l'encadrement du consentement, ainsi que son possible retrait, garantissent aux personnes un meilleur contrôle sur leurs données. En effet, le responsable du traitement devra obtenir un consentement spécifique et éclairé exprimé par un acte positif pour chaque finalité envisagée[1403]. Les difficultés pratiques entourant l'obtention d'un tel consentement risquent de remettre en cause certaines industries numériques.

Il est établi que la collecte massive et indifférenciée de données à caractère personnel opérée par le secteur privé a servi un modèle économique fondé sur la publicité ciblée[1404]. À ce propos, Madame Anne Debet se demandait justement si une interprétation stricte du consentement n'était pas susceptible de profondément remettre en cause ce modèle économique[1405]. En effet, dès lors que les individus peuvent librement choisir de fournir – ou de ne pas fournir – leurs données à caractère personnel, sans qu'un tel refus les empêche d'accéder au service, ils risquent de n'autoriser qu'un accès restreint à leurs données. Cette baisse importante de la collecte de données personnelles se confirme lorsque les utilisateurs ont une réelle capacité de choix. Par exemple, depuis une mise à jour du logiciel iOS 13 donnant aux détenteurs d'iPhone une réelle possibilité de contrôle à l'égard des données de géolocalisation transmises aux applications, 80 % des utilisateurs ont désactivé tout suivi de localisation en arrière-plan, réduisant ainsi drastiquement la collecte de ces données[1406]. Plus récemment encore, Facebook a annoncé publiquement que la mise à jour du logiciel iOS 14 qui rend le traçage des utilisateurs entre applications plus transparent

---

[1402] V. déjà sur les questions de patrimonialisation de la personne, L. Josserand, « La personne humaine dans le commerce juridique », *D.* 1932, chron. 1 ; P. Catala, « La transformation du patrimoine dans le droit civil moderne », *RTD civ.* 1966, p. 185, nº 28. Plus récemment, v. A.-F. Eyraud, *Le contrat réel. Essai d'un renouveau par le droit des biens*, th. Paris I, 2003, nº 445, p. 376 s. ; B. Edelman, « De la propriété-personne à la valeur-désir », *D.* 2004, p. 155 ; J. Antippas, « Propos dissidents sur les droits dits "patrimoniaux" de la personnalité », *RTD com.* 2012, p. 35 ; J.-M. Bruguière, « "Droits patrimoniaux" de la personnalité. Plaidoyer en faveur de leur intégration dans une catégorie des droits de la notoriété », *RTD civ.* 2016, p. 1. Plus largement sur la réification des éléments de la personnalité, v. J. Rochfeld, *Les grandes notions du droit privé*, 2e éd., PUF, 2013, *Vº* « La personne », nº 31, p. 66.

[1403] V. par ex. CNIL, décision nº 2018-042 du 30 octobre 2018 mettant en demeure la société Vectaury ; CNIL, délibération nº 2019-001 du 21 janvier 2019 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google LLC, § 156.

[1404] Madame Shoshana Zuboff a théorisé ces pratiques et les qualifie de « capitalisme de surveillance », v. S. Zuboff, *The age of surveillance capitalism : the fight for a human future at the new frontier of power,* PublicAffairs, 2019. Pour un aperçu de cette théorie, v. S. Zuboff, « Un capitalisme de surveillance », *Le Monde diplomatique* janv. 2019, p. 10.

[1405] A. Debet, « Le consentement dans le RGPD : rôle et définition », *CCE* 2018, nº 4, dossier 9.

[1406] S. Joseph, « Apple's new privacy features have further rattled the location-based ad market », *Digiday* 13 janv. 2020.

dès lors qu'il repose sur un consentement explicite, allait réduire drastiquement ses revenus publicitaires[1407]. Ainsi, beaucoup d'entreprises dont le modèle économique est fondé sur la publicité ciblée constatent une baisse importante des données collectées[1408], et une baisse conséquente de leurs revenus[1409]. Comme le remarquait déjà Monsieur Pierre-Yves Gautier en 2009, seul un principe *d'opt-in* permet une véritable protection du consommateur en matière de données personnelles[1410]. C'est un tel principe que le fondement du consentement prévu par le règlement européen permet de mettre en place et qu'il convient de garantir par la reconnaissance d'un contrat spécial.

En pratique, l'articulation entre la condition du consentement et celle du contrat reste complexe et seuls des contrôles plus fréquents assureront une application protectrice des personnes et respectueuse de la volonté du législateur.

Ainsi, le contrat spécial de traitement de données personnelles, auquel s'ajoutent d'autres principes tels que la minimisation des données et le développement de technologies protectrices de la vie privée, peut réduire la collecte effectuée par les services numériques friands de données à caractère personnel. Ces mesures ont des effets positifs sur la protection des personnes et leur offrent une meilleure maîtrise de leurs informations. Un tel pouvoir de contrôle des personnes est important pour assurer une meilleure effectivité de la protection des personnes. Il apparaît d'autant plus nécessaire que les traitements de ces données peuvent engendrer des atteintes aux personnes.

SECTION II – DES TRAITEMENTS POUVANT PORTER ATTEINTE AUX PERSONNES

377. Les risques liés aux traitements de données. La généralisation des traitements de données personnelles engendrée par la diffusion de l'informatique a amplifié les risques identifiés dès la fin des années 1960. À l'heure où ces traitements font partie

---

[1407] Facebook, « Preparing audience network for iOS 14 », 26 août 2020. Selon une enquête Tap Research, 85 % des personnes préfèreraient ne pas être tracées si elles avaient le choix, P. Haggin et J. Harwitz, « Facebook says Apple's new iPhone update will disrupt online advertising », *The Wall Street Journal* 26 août 2020.

[1408] Selon le directeur de l'entreprise Teemo, avant l'entrée en application du règlement européen, l'entreprise réussissait à obtenir près de 100 % d'*opt-in*. Depuis que les modalités d'obtention du consentement ont été renforcées, l'entreprise a constaté une baisse de 30 % du taux de consentement, v. B. Grouchko, « Les nouveaux challenges posés aux marketeurs par le RGPD », *Stratégies* 3 juill. 2019. La CNIL avait d'ailleurs mis en demeure cette entreprise, notamment pour non-respect des conditions d'obtention du consentement ; v. CNIL, décision n° 2018-022 du 25 juin 2018 mettant en demeure la société Teemo.

[1409] C. de Laubier, « Publicité en ligne : les GAFA américains n'ont pas réussi à tuer l'ex-licorne française Criteo », *Edition multimédi@* 25 févr. 2019.

[1410] P.-Y. Gautier, « Réseaux sociaux sur l'internet, données personnelles et droit des contrats », *D.* 2009, p. 616. L'*opt-in* consiste à poser un principe d'interdiction d'utilisation des données et à rendre obligatoire l'obtention d'un consentement explicite pour l'utilisation des données (par exemple, le fait de cocher une case).

de notre quotidien et rythment nos journées, la question de l'effectivité de la protection juridique se pose. Le droit des données personnelles réussit-il à atteindre l'objectif qu'il s'était fixé en 1978 et à protéger les personnes ainsi que leurs libertés ?

378. Plan. Pour savoir si le droit répond efficacement aux dangers pesant sur la protection des personnes, encore faut-il réussir à identifier les risques que l'informatique et la mise en réseau des ordinateurs font peser sur les libertés individuelles. Après avoir analysé les atteintes classiques aux personnes résultant des traitements de données à caractère personnel (§ I), il faudra s'intéresser aux nouvelles formes d'atteintes (§ II).

§ I. Les atteintes classiques aux personnes résultant des traitements de données à caractère personnel

379. Les intrusions dans l'intimité commises par la presse. Lassés de constater l'étalage dans la presse de détails intimes des familles populaires de Boston[1411], Louis Brandeis et Samuel Warren avaient proposé, dans leur emblématique article de 1890, de reconnaître un nouveau droit, jusqu'alors inconnu de la *common law* : le droit à la *privacy*. Ce droit, défini comme le droit « d'être laissé tranquille »[1412], visait à accorder aux personnes une protection juridique contre les intrusions permises par les inventions de l'époque, telles que les photographies instantanées. En France, ce sont aussi les atteintes commises par la presse qui ont contribué au développement du droit au respect de la vie privée[1413]. La protection juridique française de la vie privée s'est donc formée *via* des dispositions ponctuelles encadrant la liberté de la presse, principalement avec

[1411] Pour Madame Monique Contamine-Raynaud, la vie privée serait « une notion bourgeoise qui a pris jour à une époque où toute une classe sociale, jalouse de ses privilèges, s'enfermait à l'abri du voisin », M. Contamine-Raynaud, in *L'information en droit privé : travaux de la conférence d'agrégation,* dir. P. Lagarde, Y. Loussouarn et I. Tallon-Frouin, LGDJ, 1978, p. 405.
[1412] L. Brandeis et S. Warren, « The right to privacy », *Harvard Law Review* 1890, vol. 4, p. 193 s. [4 HARV. L. REV. 193], spéc. p. 195 s. Sur les raisons ayant poussé ces auteurs à écrire cet article, v. D. Glancy, « The invention of the right to privacy », *Arizona Law Review* 1979, vol. 21, p. 1 s. [21 ARIZ. L. REV. 1].
[1413] J.-L. Halpérin, « Diffamation, vie publique et vie privée en France de 1789 à 1944 », *Droit et cultures* 2013, vol. 63, p. 145 s. ; P. Kayser, « Les droits de la personnalité, aspects théoriques et pratiques », *RTD civ.* 1971, p. 445, n° 43. Sur les interactions modernes entre liberté de la presse et droits de la personnalité, v. J.-P. Gridel, « Liberté de la presse et protection civile des droits modernes de la personnalité en droit positif français », *D.* 2005, p. 391 ; *Rép. civ.* Dalloz, *V°* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), n^os^ 205 s.

les lois de 1819[1414], de 1868[1415] et de 1881[1416]. Le droit au respect de la vie privée s'est construit comme une limite au droit de la presse[1417].

380. Les captations et représentations d'image. C'est également à la suite des intrusions dans l'intimité des familles commises par la presse que le droit à l'image a reçu une reconnaissance juridique en France. Ce droit est apparu dans une décision de 1858 par laquelle le tribunal de la Seine condamnait la reproduction dans la presse d'un dessin représentant Rachel, célèbre actrice de l'époque, sur son lit de mort[1418]. Pour le tribunal, seule la volonté de la famille, extériorisée par un consentement formel, aurait pu justifier une telle reproduction, et en l'absence de celle-ci, la reproduction de l'image était illicite[1419].

381. La reconnaissance d'un droit de contrôle sur les informations personnelles. En reconnaissant aux personnes le pouvoir d'autoriser, ou non, la diffusion de leur image (ou de celle d'un parent défunt), le tribunal de la Seine reconnaissait ce qui a ensuite été théorisé comme le droit de contrôle à l'égard des informations personnelles[1420]. La doctrine américaine a été la première à théoriser la *privacy* comme un tel pouvoir de contrôle[1421]. Par exemple, Alan Westin considérait que la *privacy* est « la possibilité pour des individus, groupes et institutions de déterminer pour eux-

---

[1414] Loi du 17 mai 1819, *B.* 278 nº 6444 ; loi du 26 mai 1819, *Moniteur Universel*, 14 juin 1819, p. 782, nº 165 ; et loi du 9 juin 1819, *B.* 284, nº 6648 et nº 6649. Si l'expression « vie privée » n'apparaît pas dans la loi, elle a été amplement discutée à l'occasion des débats parlementaires. Le discours du député Royer-Collard du 27 avril 1819 est d'ailleurs resté célèbre. Il avait proclamé que « Il n'est pas permis de dire la vérité sur la vie privée. Voilà la disposition principale, le reste est une exception… Voilà donc la vie privée murée, si je puis me servir de cette expression ; elle est déclarée invisible, elle est renfermée dans l'intérieur des maisons », v. P.-P. Royer-Collard, *De la liberté de la presse*, Librairie de Médicis, 1949, p. 24 s.

[1415] Loi nº 15-979 du 11 mai 1868 relative à la presse, *D.* 1868, IV, p. 62. Son article 11 prévoyait que « toute publication dans un écrit périodique relative à un fait de la vie privée constitue une contravention punie d'une amende de cinq cents francs. La poursuite ne pourra être exercée que sur la plainte de la partie intéressée ».

[1416] Loi du 29 juill. 1881 sur la liberté de la presse, *JORF* 30 juill. 1881, nº 206, p. 4201. Dans sa version initiale, la loi de 1881 ne faisait pas référence à la notion de vie privée et s'inscrivait donc en rupture avec la continuité législative, v. J.-L. Halpérin, « L'essor de la "privacy" et l'usage des concepts juridiques », *Droit et Société* 2005, nº 61, p. 765 s., spéc. 772. C'est l'ordonnance du 6 mai 1944 qui réintroduit ce terme, ordonnance du 6 mai 1944 relative à la répression des délits de presse, *JORF* 20 mai 1944, nº 0042, p. 402.

[1417] Sur cette opposition, v. J.-L. Halpérin, « Protection de la vie privée et privacy : deux traditions juridiques différentes ? », *Les Nouveaux Cahiers du Conseil constitutionnel* 2015, nº 48, p. 59.

[1418] Trib. Seine, 16 juin 1858, *Rachel*, *D.* 1858, III, p. 62.

[1419] Trib. Seine, 16 juin 1858, *Rachel*, *D.* 1858, III, p. 62.

[1420] V. not. l'article premier de la loi nº 78-17 du 6 janv. 1978 et le considérant 7 du règlement UE nº 2016/679 qui reconnaissent aux personnes concernées un *pouvoir de contrôle* à l'égard de leurs données.

[1421] V. not., L. Brandeis et S. Warren, « The right to privacy », *Harvard Law Review* 1890, vol. 4, p. 193 s. [4 HARV. L. REV. 193] ; C. Fried, « Privacy », *Yale Law Journal* 1968, vol. 77, p. 475 s. [77 YALE L.J. 475], spéc. p. 482 ; C. Fried, *An anatomy of values : problems of personal and social choice*, Harvard University Press, 1970, p. 140 ; R. Parker, « A definition of privacy », *Rutgers Law Review* 1974, vol. 27, p. 275 s. [27 RUTGERS. L. REV. 275] ; A. Allen, « Privacy-as-data control : conceptual, practical and moral limits of the paradigm », *Connecticut Law Review* 1999, vol. 32, p. 861 s. [32 CONN. L. REV. 861], spéc. p. 862 s. ; A. Moore, « Defining privacy », *Journal of Social Philosophy* 2008, vol. 39, p. 411 s. [39 J. SOC. PHILOS. 411].

mêmes quand, comment et jusqu'à quel point des informations personnelles les concernant peuvent être communiquées à des tiers »[1422]. La doctrine française a repris cette théorie en considérant le pouvoir de contrôle comme l'une des prérogatives du droit français au respect de la vie privée[1423]. Les risques liés à la mise en mémoire informatique des informations personnelles et à leur utilisation ont accentué ce besoin de contrôle des personnes à l'égard de leurs données personnelles.

382. Les risques liés à la mémorisation informatique. C'est dans les années 1960, avec la diversification des tâches effectuées par les ordinateurs, que la question de la protection des données enregistrées par ces machines a commencé à se poser. Initialement, seules les administrations et les grandes entreprises pouvaient s'offrir ces assistants utiles, notamment pour des raisons de budget et de place[1424]. L'apparition des ordinateurs personnels et leur diffusion progressive au grand public à la fin des années 1970 ont modifié en profondeur la manière dont les humains traitent l'information, notamment celle relative aux personnes[1425]. Les fiches perforées cèdent la place aux bases de données rendant l'accès, le traitement et la conservation des données plus rapides et plus simples. Le développement des réseaux contribue aux transferts des bases de données entre les pays, et les moteurs de recherche facilitent les opérations de croisement et de synthèse de fichiers[1426]. Rapidement, l'informatique n'est plus réservée à une élite, elle se répand partout : dans les banques, dans les entreprises, dans les foyers... Cette diffusion de l'informatique banalise la collecte d'informations nominatives. Pourtant, les risques induits par ces enregistrements et mémorisations sont considérables. Contrairement au cerveau humain, la mémoire d'un ordinateur n'oublie pas : la conservation informatique prolonge donc la durée de traitement et de

---

[1422] A. Westin, *Privacy and Freedom*, Ig Publishing, 1968, réimpr. 2015, p. 5. Dans le même sens, Monsieur Arthur Miller définit la *privacy* comme « la capacité pour un individu de contrôler la circulation des informations le concernant », A. Miller, *Assault on Privacy, Computers, Data Banks, and Dossiers*, The University of Michigan Press, 1971, p. 40.

[1423] *Rép. civ.* Dalloz, *V°* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), n^os^ 21 s. ; D. Gutmann, *Le sentiment d'identité. Étude de droit des personnes et de la famille*, th. Paris II, 2000, LGDJ, n° 328, p. 277 ; J.-C. Saint-Pau, « La distinction des droits de la personnalité et de l'action en responsabilité civile », in *Mélanges H. Groutel*, Litec, 2006, p. 405 s., n° 9, spéc. p. 411 s.

[1424] Comme le remarquait déjà Monsieur Michel Volle en 1999, « 50 ans séparent le premier ordinateur (50 tonnes, 25 kW, quelques milliers de positions de mémoire, cent instructions par seconde) du microprocesseur Pentium (quelques grammes, 25 watts, 8 à 32 Megaoctets de mémoire, 100 MIPS). L'évolution n'est pas terminée : la loi de Moore (…) se vérifie depuis le début des années 70. Les chercheurs pensent qu'elle jouera jusque vers 2010 », v. M. Volle, *Économie des nouvelles technologies. Internet, télécommunications, informatique, audiovisuel, transport aérien*, Economica, 1999.

[1425] V. sur l'évolution du traitement des informations du recensement aux États-Unis, v. Census Bureau, « A monograph on confidentiality and privacy in the U.S. census », 2001.

[1426] G. Braibant, « Données personnelles et société de l'information. Rapport au Premier ministre sur la transposition en droit français de la directive n° 95/46 », La Documentation française, 1998, p. 1.

sauvegarde des informations[1427]. Par ailleurs, l'informatique permet de traiter les informations bien plus rapidement et efficacement qu'un humain. À ces éléments s'ajoute la possibilité d'interconnecter des fichiers se trouvant à des endroits différents, faisant ainsi peser des risques nouveaux de centralisation des informations. L'ensemble de ces facteurs ont démultiplié les risques d'atteintes aux personnes. Ainsi, c'est parce que les ordinateurs sont capables de manier de très grandes quantités de données, dans des temps inédits, que les risques liés à leur utilisation ont augmenté.

383. Le développement d'une société de surveillance. Tous ces éléments ont favorisé le développement d'une société de surveillance et de contrôle, se rapprochant dangereusement de celle dépeinte par Georges Orwell dans son roman emblématique *1984*[1428] ou des mécanismes de surveillance retracés par les philosophes Michel Foucault[1429] et Gilles Deleuze[1430]. Ces nouvelles modalités de traitement de l'information font peser des risques inédits sur la vie privée puisqu'elles rendent possible une surveillance diffuse, généralisée et à faible coût. Une telle normalisation de la surveillance n'atténue pas pour autant ses effets qui, selon certains auteurs, seraient comparables à ceux des barreaux d'une prison[1431]. Ce n'est sans doute pas un hasard si les frères Bentham ont appliqué le concept de Panoptique aux établissements devant surveiller les personnes, notamment aux prisons. La spécificité de ce bâtiment circulaire était de permettre l'observation à tout moment des faits et gestes des détenus grâce à une vision totale sur l'ensemble des cellules[1432]. Lorsque Foucault transpose l'analyse de la structure du Panoptique à l'organisation sociale, celle-ci en ressort métamorphosée en une société disciplinaire axée sur le contrôle social. Foucault remarque que la sensation de visibilité induite par la structure du Panoptique assure le fonctionnement automatique du pouvoir : la surveillance est permanente dans ses effets, même si elle est discontinue dans son action[1433]. Confirmant ces analyses, de nombreuses études effectuées en sciences sociales ont montré que le sentiment d'être sous surveillance a d'importants effets sur la santé, tant physique que morale, et

---

[1427] Sur le droit à l'oubli, v. *infra*, n^os^ 406 s.
[1428] G. Orwell, *1984,* Gallimard, 1950.
[1429] M. Foucault, *Surveiller et punir. Naissance de la prison*, Gallimard, 1975, p. 202 s.
[1430] G. Deleuze, « Post-scriptum sur les sociétés de contrôle », *Pourparlers* 1990.
[1431] « A man without privacy is a man without dignity ; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars », Z. Cowen, *The private man*, The Boyer Lectures Australian Broadcasting Commission, 1969, p. 9 s.
[1432] J. Bentham, *Panopticon or the inspection house*, vol. 1, Payne, 1791, p. 63.
[1433] M. Foucault, *Surveiller et punir. Naissance de la prison*, Gallimard, 1975, p. 234.

engendre des sentiments de faible estime de soi, de dépression et d'anxiété[1434]. C'est notamment pour encadrer ces risques que les législations relatives aux données à caractère personnel se sont développées.

384. L'adoption des législations protégeant les données personnelles. Plusieurs principes permettent de répondre aux risques liés au développement de cette société de surveillance. Par exemple, le principe de transparence, interdisant la collecte secrète des données ; le principe de pertinence, encadrant les finalités des traitements ; le principe de sécurité, prescrivant l'obligation de protéger les données contre des accès par des tiers ; et les droits des personnes sur leurs données[1435]. La loi du 6 janvier 1978 reconnaissait ainsi aux personnes concernées plusieurs droits pour qu'elles gardent le contrôle sur leurs informations, notamment le droit d'accès, le droit d'opposition, ou le droit de mettre à jour les données[1436]. La volonté de garantir un droit de contrôle aux personnes concernées est si centrale qu'en 2016, les législateurs européen et français l'ont érigé en principe général de la matière[1437]. Cette prérogative de contrôle se rapproche du concept allemand d'autodétermination informationnelle.

385. L'autodétermination informationnelle, un principe en rapport avec le pouvoir de contrôle. Le droit à l'autodétermination informationnelle a été consacré par la Cour constitutionnelle fédérale allemande dans un arrêt du 15 décembre 1983[1438]. La juridiction allemande l'avait défini comme « le pouvoir de l'individu de décider lui-même, sur la base du concept d'autodétermination, quand et dans quelle mesure une information relevant de sa vie privée peut être communiquée à autrui »[1439]. Pour

---

[1434] B. Schneier, *Data and Goliath : The hidden battles to collect your data and control your world*, Norton & Company, 2015, p. 127.
[1435] V. not. United States Department of Health, Education and Welfare, « Records, computers, and the rights of citizens », 1973, p. 40 s. ; OCDE, Lignes directrices du 23 sept. 1980 sur la vie privée et les flux transfrontières de données à caractère personnel.
[1436] Sur les droits reconnus aux personnes, v. P. Kayser, *La protection de la vie privée*, 2e éd., Economica, 1990, nos 289 s., p. 367 s.
[1437] L'article 54 de la loi no 2016-1321 du 7 octobre 2016 pour une République numérique a complété l'article 1er de la loi Informatique et libertés par une phrase prévoyant que « Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi ». Le législateur européen a, quant à lui, proclamé dans le considérant 7 du règlement UE no 679/2016 que « Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant ».
[1438] BVerfGE 65, 1 – Volkszählung Urteil des Ersten Senats vom 15 Dezember 1983, pour une analyse de l'arrêt en français, v. Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », in *État de droit et virtualité*, dir. K. Benyekhlef et P. Trudel, Thémis, 2009, p. 157 s. Pour une analyse des précédents arrêts ayant conduit à cette reconnaissance, v. C. Koumpli, *Les données personnelles sensibles. Contribution à l'évolution du droit fondamental à la protection des données à caractère personnel*, th. Paris I, 2019, p. 100 s.
[1439] BVerfGE 65, 1 – Volkszählung Urteil des Ersten Senats vom 15 Dezember 1983.

certains auteurs, ce principe établit une conception renouvelée du rapport de la personne avec ses données, puisque chaque individu bénéficierait d'une véritable autonomie dans leur gestion[1440]. En France, le Conseil d'État a reconnu dans son rapport sur *Le numérique et les droits fondamentaux* l'intérêt de ce concept, tout en rappelant que « la seule affirmation de ce droit ne permet pas de le rendre effectif et les instruments de la protection des données doivent être profondément transformés pour y parvenir »[1441]. Ainsi, le droit français des données personnelles reconnaît, au travers de plusieurs prérogatives, un pouvoir de contrôle à l'égard des données, mais celui-ci n'englobe pas complètement un droit à l'autodétermination informationnelle. Ce pouvoir de contrôle suffit-il à protéger de manière efficace les personnes contre les nouvelles formes d'atteintes aux personnes issues des traitements de données personnelles ?

§ II. Les atteintes nouvelles aux personnes résultant des traitements de données à caractère personnel

386. Plan. Il est courant d'affirmer que les traitements de données à caractère personnel sont intrusifs (A). Pour mieux circonscrire les risques engendrés par ces traitements intrusifs sur les personnes, il convient de reconnaître une liberté d'autodétermination (B).

A. Des traitements intrusifs

387. L'explosion des quantités de données produites, facilitant un traçage des personnes sans précédent. Le numérique, réservé pendant plusieurs décennies à une communauté d'experts, s'est amplement popularisé. L'avènement du Web 2.0 acte le passage d'un web statique au web social, dans lequel la dimension de partage et d'échange d'informations est centrale. L'explosion du nombre d'utilisateurs engendre une surabondance des données produites, et les risques identifiés au début du développement de l'informatique sont amplifiés.

[1440] J. Rochfeld, « Données personnelles : quels nouveaux droits ? », *Statistiques et société* 2017, vol. 5, nº 1, p. 47.
[1441] Conseil d'État, « Le numérique et les droits fondamentaux », *Rapport Public 2014*, La Documentation française, 2014, p. 267.

Progressivement, tout devient quantifiable et quantifié, nos moindres actions sont traduites en données pour ensuite être analysées[1442]. Chaque pas, chaque activité physique, chaque site consulté, génère désormais des données. Une fois consignées dans une base, ces données sont ensuite traitées pour produire un nouveau savoir sur la personne : c'est l'arrivée du Web 3.0, centré autour de l'humain et de la personnalisation de contenus[1443]. Les algorithmes rythment, plus que jamais, les contenus visionnés, les trajets empruntés, les musiques écoutées et les restaurants choisis.

388. L'explosion des producteurs de données. Longtemps élément central de la collecte d'informations personnelles, l'ordinateur partage depuis près de deux décennies cette attribution avec les *smartphones*. Le lancement de l'iPhone en 2007 acte définitivement l'entrée de ces micro-ordinateurs dans nos vies quotidiennes. De petite taille et avec de multiples fonctionnalités, ils se déplacent avec leurs détenteurs et permettent une collecte de données en continu. Ils ont ainsi contribué à l'augmentation de données collectées, mais surtout à leur diversité, leur qualité et leur précision. Tels de véritables petits mouchards dans nos poches, les *smartphones* permettent de collecter un nombre considérable de données. La moindre seconde d'attente est désormais occupée par ce petit écran : on lève un pouce pour montrer son approbation, on envoie un message à l'être aimé pour dire que nous rapportons du vin pour le dîner, on prend une photo du coucher de soleil pour la publier sur les réseaux sociaux, on utilise son application de navigation connectée pour trouver la route la plus rapide[1444]. Toutes ces actions, en apparence parfaitement anodines, laissent d'invisibles petites traces, permettant ensuite de dresser un portrait de l'utilisateur[1445].

Avec la mise en réseau des ordinateurs, puis le développement du *big data*, les responsables du traitement ont préféré centraliser les données sur leurs serveurs afin

---

[1442] D. Cardon, *À quoi rêvent les algorithmes : nos vies à l'heure des big data,* Seuil, 2015, p. 7.
[1443] Pour une présentation de l'évolution du Web, v. O. Le Deuff, « Du web 2.0 à l'Arcadie », *URFIST Info* 2007.
[1444] Selon une opinion doctrinale récente, le droit devrait également protéger l'attention, v. C. Zolynski, M. Le Roy et F. Levin, « L'économie de l'attention saisie par le droit », *Dalloz IP/IT* 2019, p. 614. Sur la transformation apportée par Internet dans la production de contenus en ligne et le déluge d'informations auquel les personnes sont désormais confrontées, v. E. Pariser, *The filter bubble,* Penguin Press, 2011, p. 32. Pour une étude des frontières entre la productivité et la distraction, v. S. Genner, « ON / OFF. Risks and rewards of the anytime-anywhere Internet », University of Zurich, 2015, p. 57.
[1445] Sur le traçage des personnes, v. J. Rochfeld, « La vie tracée ou le code civil doit-il protéger la présence numérique des personnes », in *Mélanges J. Hauser*, Dalloz, 2012, p. 619 s., nº 1, spéc. p. 619 s. Sur le recours au *data mining* aux fins de profilage, v. not. Y. Poullet, *La vie privée à l'heure de la société numérique,* Larcier, 2019, nº 13, p. 29 s. Sur l'encadrement du profilage par le règlement européen, v. G29, WP 251 rév. 01, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, 6 févr. 2018, p. 5 s.

d'effectuer de l'apprentissage automatique. Cette centralisation était nécessaire parce que le développement des modèles exigeait une puissance de calcul plus large que celle disponible sur l'appareil de l'utilisateur. Pour autant, cette centralisation des données présente d'importants risques, tant en matière de sécurité qu'en matière de protection de la vie privée. Au cours de la dernière décennie, l'augmentation de la puissance de calcul disponible sur les *smartphones* a permis de mettre en œuvre les traitements d'apprentissage directement sur l'appareil de l'utilisateur, réduisant ainsi la quantité d'informations transférées aux responsables du traitement, tout en permettant d'améliorer le modèle grâce à l'envoi de statistiques agrégées[1446]. Pour autant, cette pratique est loin d'être diffuse et la centralisation des données demeure le modèle dominant.

En plus des *smartphones,* de nombreux autres objets connectés[1447] envahissent notre quotidien et collectent toujours plus de données sur nos vies : l'œuf minuteur de la cuisine est remplacé par un assistant vocal « intelligent »[1448], la poupée en porcelaine est remplacée par la poupée connectée, et la montre connectée enregistrant chaque battement de notre cœur a succédé à la montre analogique. Ces objets envahissent nos foyers et affinent, grâce aux données qu'ils collectent, les traits de nos vies. Pour le dire simplement, les données sont générées tout le temps et stockées partout.

Le nombre de traces, leur variété et leur précision favorisent ainsi l'émergence d'un modèle de société fondé sur le prédictif et la personnalisation : la société de surveillance est alors couplée à celle de manipulation. C'est effectivement l'un des dangers liés à l'expansion des traitements de données et à la diffusion des traitements de données personnalisés. Le droit des données à caractère personnel est confronté à de nouveaux défis qui l'invitent à se transformer afin de protéger de manière effective les personnes contre une société de manipulation.

[1446] La technique d'apprentissage fédéré est utilisée pour améliorer la qualité des dictionnaires d'auto-correction sur les *smartphones,* K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal et K. Seth, « Privacy secure agregation for privacy-preserving machine learning », *CCS'* oct. 2017, Dallas.

[1447] L'objet connecté est classiquement défini comme « un dispositif matériel permettant de collecter, stocker, transmettre et traiter des données issues du monde physique », v. E. Daoud et F. Plénacoste, « Cybersécurité et objets connectés », *Dalloz IP/IT* 2016, p. 409.

[1448] Les assistants vocaux, notamment ceux de Google (Echo), Amazon (Alexa) et Apple (Siri), ont fait l'objet de polémiques quant aux enregistrements des interactions, à leur transmission et à leur écoute par des employés de ces entreprises, v. pour un bref résumé N. Six, « Avec des enceintes connectées, des conversations loin d'être privées », *Le Monde* 12 avr. 2019. Sur ce sujet, v. CNIL, « À votre écoute. Exploration des enjeux éthiques, techniques et juridiques des assistants vocaux », Livre Blanc, nº 1, 2020.

389. Une personnalisation des services. La collecte croissante de données entraîne une meilleure connaissance des personnes, laquelle facilite ensuite leur manipulation[1449]. Cette collecte de données n'est que la première étape d'un processus complexe : les données sont ensuite consignées dans de gigantesques bases de données afin de leur appliquer des méthodes de traitement visant à inférer de nouvelles informations sur les personnes[1450]. Dès 1978, le législateur s'était montré très frileux à l'égard des décisions prises sur le fondement des traitements automatisés en consacrant, dans les premiers articles de la loi, des dispositions visant à les encadrer et à les interdire[1451]. Cette interdiction se limitait toutefois aux seules décisions de justice et à quelques décisions administratives ou privées[1452]. En effet, le législateur de 1978 ne pouvait pas anticiper l'ampleur des traitements à venir, ni leurs effets sur la liberté de la vie privée.

La liberté de la vie privée est définie comme un ensemble de possibilités d'actions infinies qui « constituent des phénomènes de non-droit (lire tel livre ou tel autre, porter des chaussettes bleues ou vertes, se réveiller tôt ou tard…) ; elles n'entrent dans le domaine juridique que pour déterminer leurs limites et donc leur degré de protection (l'ordre public ou un tiers prétendent m'interdire le port de chaussettes bleues : j'avance alors un droit au respect de la liberté) »[1453]. Mais, qu'en est-il lorsqu'un tiers ne vient pas m'interdire de porter des chaussettes bleues, mais me manipule pour que je porte des chaussettes vertes ? La question de la mise en œuvre de la liberté de la vie privée trouve un écho particulier lorsque des traitements opérés sur des données personnelles visent à manipuler la personne afin qu'elle adopte un certain comportement. Madame Judith Rochfeld évoquait précisément ces risques en considérant que « dès lors qu'il devient possible […] de prédire nos comportements, il est également possible de les orienter : de nouveaux modes d'influence se développent

---

[1449] Sur l'évolution des déterminismes sociologiques des comportements et des opinions, v. D. Cardon, *À quoi rêvent les algorithmes : nos vies à l'heure des big data,* Seuil, 2015, p. 47 s. citant P. Bourdieu, *La distinction. critique sociale du jugement*, Minuit, 1979.

[1450] Le volume de données collectées donne du sens à des informations apparaissant pourtant, à première vue, très anodines ou clairsemées, v. P. Delort, *Le big data*, 2e éd., PUF, 2018, p. 29 ; Y. Poullet, *La vie privée à l'heure de la société numérique,* Larcier, 2019, no 13, p. 29 s.

[1451] L'article 2 de cette loi interdisait les décisions de justice, administrative ou privée impliquant une appréciation sur un comportement humain fondée sur un traitement automatisé d'informations (notamment lorsqu'il est fondé sur un profil ou une analyse de la personnalité de l'intéressé). L'article 3 garantissait aux personnes le droit de connaître et contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats leur sont opposés. Ces principes avaient été repris dans l'article 10 de la loi no 78-17 du 6 janvier 1978 telle que modifiée par la loi no 2004-801 du 6 août 2004.

[1452] V. *infra*, no 450.

[1453] J.-C. Saint-Pau, « La distinction des droits de la personnalité et de l'action en responsabilité civile », in *Mélanges H. Groutel*, Litec, 2006, p. 404 s., no 9, spéc. p. 412 ; P. Kayser, *La protection de la vie privée par le droit*, 3e éd., Economica, 1995, nos 18 s., p. 45 s.

dont nous n'avons pas toujours pleinement conscience »[1454]. Ainsi, ce sont notamment les techniques liées au profilage qui rendent possibles de telles manipulations.

390. L'atteinte à la liberté personnelle par le profilage. Le profilage est un traitement consistant à utiliser des données à caractère personnel pour évaluer, par le biais d'analyses ou de prédictions, certains aspects personnels d'une personne physique[1455]. Lorsqu'elle est profilée, la personne est enfermée dans des catégories générales de comportement afin de prédire, à l'avance, ses agissements futurs. Schématisée et objectivée de la sorte, la personne se voit nier l'existence d'un libre arbitre et de la faculté d'agir différemment des autres dans une même situation[1456]. Le profil instaure donc une forme de déterminisme incompatible avec l'attribut le plus précieux de la liberté : le choix d'un futur autodéterminé[1457]. Avec cette conception de la personne, on nie les qualités qui font d'elle un être humain[1458].

À ce stade de l'analyse, deux observations peuvent être formulées : d'une part, la tendance de l'homme à vouloir quantifier les choses pour éviter l'imprévisibilité, le pousse à recourir à des outils (notamment informatiques et numériques) l'aidant à mieux anticiper et prédire l'avenir, et d'autre part, les algorithmes de profilage présentent le risque de nier la complexité du comportement humain en enfermant la personne dans un carcan trop rigide de choix prédéfinis[1459]. Ces outils sont souvent loin d'être neutres pour les personnes, puisqu'ils peuvent avoir d'importantes implications sur l'autonomie individuelle (en considérant que la personne va agir de la même façon

---

[1454] J. Rochfeld, « Contre l'hypothèse de la qualification des données personnelles comme des biens », in *Les biens numériques,* dir. E. Netter et A. Chaigneau, CEPRISCA, 2015, p. 221 s., n° 4, spéc. p. 225.

[1455] L'article 4 du règlement UE n° 2016/679 définit le profilage comme « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».

[1456] J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 184 ; S. Merabet, *Vers un droit de l'intelligence artificielle,* th. Aix-Marseille, 2018, Dalloz, n^{os} 246 s., p. 238 s.

[1457] F. Rigaux, *La protection de la vie privée et les autres biens de la personnalité,* Bruylant, 1990, n° 537, p. 597 s.

[1458] D'ailleurs, pour Emmanuel Mounier, « la personne est ce qui ne peut être répété deux fois », E. Mounier, *Le personnalisme,* PUF, 2010, p. 49. Monsieur Guillaume Lécuyer affirmait également qu'au-delà de son appartenance à l'humanité, l'individu est un être unique c'est-à-dire différent de son prochain, v. G. Lécuyer, *Liberté d'expression et responsabilité. Étude de droit privé,* th. Paris I, 2006, n° 4, p. 5.

[1459] V. not. J. Rochfeld, « La vie tracée ou le code civil doit-il protéger la présence numérique des personnes », in *Mélanges J. Hauser*, Dalloz, 2012, p. 619 s., n° 10, spéc. p. 630. Dans cet article, Madame Judith Rochfeld rappelle l'importance des algorithmes derrière les traces laissées par les personnes sur Internet. Madame Antoinette Rouvroy critique aussi ces catégorisations automatiques en rappelant que les « opérations de *datamining* et de profilage n'apparaissent objectives et égalitaires que dans le mesure où l'on ignore qu'elles sont aveugles et sourdes à tout ce qui, du monde – les idiosyncrasies individuelles, les raisons des actions – ne se laisse pas traduire sous une forme numérique », v. A. Rouvroy, « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data », in Conseil d'État, « Le numérique et les droits fondamentaux », *Rapport Public 2014*, La Documentation française, 2014, p. 416.

qu'une autre personne placée dans la même situation), et qu'ils tendent à reproduire les biais et renforcer les discriminations[1460].

Ces techniques sont largement utilisées par le secteur privé qui a recours, notamment au sein des compagnies d'assurance et des établissements bancaires, à des systèmes de *scoring*[1461]. D'autres branches du secteur privé, notamment les entreprises présentes sur Internet, utilisent également le profilage pour influencer leurs utilisateurs. Les risques liés à la manipulation sont, avec les traitements automatisés de données, accrus.

391. Des traitements effectués à des fins de manipulation. Une part croissante de la doctrine anglo-saxonne s'intéresse aux interactions entre le droit et la manipulation. Cette dernière est définie comme l'action par laquelle on cherche à influencer l'opinion, les décisions, la conduite d'une ou plusieurs personnes, à des fins non avouées et par des moyens détournés[1462]. Déjà en 1999, Messieurs Jon Hanson et Douglas Kysar expliquaient que le format de l'information et le pouvoir de présentation des choix ont un rôle conséquent dans la prise de décision[1463]. Ceux qui réussissent à influencer les biais cognitifs[1464] ont le pouvoir de manipuler les personnes dans leurs décisions et sont donc investis d'un *pouvoir d'influence*. Si la manipulation est un trait fondamental des interactions humaines[1465], les pratiques numériques ont modifié en

---

[1460] White House, « Big data : a report on algorithmic systems, opportunity and civil rights », *Executive office of the President* mai 2016 ; v. aussi, J. Angwin, J. Larson, S. Mattu et L. Kirchner, « Machine bias. There's software used across the country to predict future criminals. And it's biased against blacks », *ProPublica* 23 mai 2016. Plus récemment aux États-Unis, 27 organisations ont signé une lettre ouverte à destination de la FTC pour l'inviter à prendre en compte les effets des pratiques de politiques de personnalisation de données sur les biais et discriminations, v. Working group, « Letter to FTC : data, biais, and disparate impact », 18 sept. 2020. Le Conseil de l'Europe s'est également intéressé à ces questions, v. not. F. Zuiderveen Borgesius, « Discrimination, artificial intelligence and algorithmic decision-making », Conseil de l'Europe 2018. Pour des travaux sur le droit français, v. not., J. Charpenet et C. Lequesne Roth, « Discrimination et biais genrés. Les lacunes juridiques de l'audit algorithmique », *D.* 2019, p. 1852.

[1461] La CNIL avait d'ailleurs adopté une autorisation unique pour les traitements mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit, CNIL, délibération nº 2006-019 du 2 février 2006 portant autorisation unique de certains traitements de données à caractère personnel mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit (décision d'autorisation unique n° AU-005).

[1462] *Dictionnaire de l'Académie française*, 9e éd., *Vo* « Manipulation », sens 4.

[1463] J. Hanson et D. Kysar, « Taking behavioralism seriously : the problem of market manipulation », *New York University Law Review* 1999, vol. 74, p. 630 s. [74 N.Y.U L. Rev. 630], spec. p. 635.

[1464] La nature des biais cognitifs est le plus souvent définie comme des tendances à produire des croyances ou des jugements erronés en vertu du fait qu'ils violent certaines règles de raisonnement, M. van Loon, « Biais cognitifs », in *L'Eycyclopédie philosophique*, dir. M. Kristanek. D'ailleurs des études se sont intéressées à l'influence du design des bandeaux de cookies sur l'obtention du consentement, v. not. C. Utz, M. Degeling, S. Fahl, F. Schaub et T. Holz, « (Un)informed consent : studying GDPR consent notices in the field », *CCS'* nov. 2019, Londres ; M. Nouwens, I. Liccardi, M. Veale, D. Karger et L. Kagal, « Dark patterns after the GDPR : scraping consent pop-ups and demonstrating their influence », *CHI'* avr. 20, Honolulu.

[1465] Sur les pouvoirs de manipulation, v. R.-V. Joule et J.-L. Beauvois, *Petit traité de manipulation à l'usage des honnêtes gens*, PUG, 1987, réimpr. 2014.

profondeur ses méthodes, formes et effets[1466]. La capacité de personnaliser les contenus, de les adapter en fonction des expériences précédentes, ainsi que les outils d'analyse de données permettent des formes de persuasion révolutionnaires[1467]. Le numérique rend cette manipulation invisible pour la plupart des utilisateurs. Plusieurs exemples illustrent ces influences et les risques qu'elles engendrent pour la protection des personnes.

392. Une utilisation des données à des fins manipulatrices, illustrations. En 2014, Facebook a reconnu avoir manipulé les informations visibles par certains de ses utilisateurs pour étudier le phénomène de « contagion émotionnelle ». Deux ans plus tôt, Facebook avait autorisé des chercheurs à afficher dans le fil d'actualité de certains utilisateurs des publications tantôt positives tantôt négatives en vue d'analyser le résultat produit sur leurs émotions[1468]. Une telle étude illustre bien les effets des traitements de données et leur impact sur les personnes : notre humeur devient un objet malléable au gré de la curiosité des responsables du traitement[1469].

Dans un autre domaine, l'algorithme de recommandations de vidéos de YouTube illustre également les effets négatifs de certains traitements de données à caractère personnel. L'un des principaux objectifs de l'algorithme de YouTube[1470] est de retenir le plus longtemps possible l'utilisateur sur le site, afin de lui montrer de la publicité et d'augmenter les revenus publicitaires de la plateforme[1471]. Pour réaliser cet objectif, l'algorithme fait évoluer graduellement l'intensité des vidéos qu'il recommande[1472]. L'utilisateur se voit ainsi proposer des vidéos confirmant son opinion

---

[1466] C. Sunstein, « Fifty shades of manipulation », *Journal of Marketing Behavior* 2016, vol. 1, p. 213 s. [1 J. MARKETING BEHAV. 213] spéc. p. 244.
[1467] T. Zarsky, « Privacy and manipulation in the digital age », *Theoretical Inquiries in Law* 2019, vol. 20, p. 158 s. [20 THEOR. INQ. LAW 158], spéc. p. 169.
[1468] A. Kramer, J. Guillory et J. Hancock, « Experimental evidence on massive-scale emotional contagion through social networks », *Proceedings of the National Academy of Sciences of the United States of America* 2014, vol. 111, p. 8788 s. [111 PROC. NATL. ACAD. SCI. USA 8788].
[1469] R. Schroeder, « Big data and the brave new world of social media research », *Big Data and Society* 2014.
[1470] Pour une analyse de l'algorithme fournie par trois employés de l'entreprise Google, v. P. Covington, J. Adams et E. Sargin, « Deep neural networks for YouTube recommandations », *RecSys* sept. 2016. V. déjà en 2010 plusieurs employés de Google avaient également publié un article sur le système de recommandation de YouTube, v. J. Davidson, B. Liebald, J. Liu, P. Nandy et T. Van Vleet, « The YouTube video recommandation system », *RecSys* sept. 2010.
[1471] Selon Monsieur Guillaume Chaslot, ancien employé de Google, YouTube gagnerait environ 1 centime d'euro par heure de visionnage pour chaque utilisateur. Sur ce sujet, v. les travaux de la plateforme AlgoTransparency.
[1472] M. Ledwich et A. Zaitsev, « Algorithmic extremism : examining YouTube's rabbit hole of radicalization », *Frist Monday* 25 févr. 2020.

ou du contenu sensationnel ou radical[1473]. Selon le *New York Times,* 70 % du temps de visionnage sur YouTube serait choisi par l'algorithme de recommandation[1474].

Ces deux exemples illustrent les défis modernes auxquels le droit des données à caractère personnel doit répondre pour garantir une protection réelle des personnes.

B. La reconnaissance de la liberté d'autodétermination

393. La liberté d'autodétermination. Pendant plusieurs décennies, le droit à l'autonomie personnelle permettait d'ériger la vie privée comme une valeur sociale protégeant la personne contre la société de surveillance[1475]. Bien que ce droit soit défini largement par la CEDH qui l'entend comme « le droit de mener sa vie comme on l'entend avec un minimum d'ingérence »[1476], il a désormais besoin d'évoluer afin de protéger les personnes contre une société de manipulation. L'augmentation considérable du nombre de traitements, la banalisation du profilage et de la personnalisation des services contribuent à dessiner une représentation très précise des personnes, permettant ensuite de mieux les influencer. Ce n'est pas seulement l'autonomie individuelle qui est atteinte par ces traitements, puisqu'en apparence, les personnes peuvent toujours agir comme bon leur semble ; c'est l'essence même de leur capacité d'agir librement qui est touchée. Épiée, profilée et influencée, la personne peut-elle encore former librement ses désirs et sa volonté ?

394. Théories philosophiques. Les théories philosophiques autour du concept de libre arbitre et de liberté sont éclairantes. Par exemple, Monsieur Robert Kane, philosophe analytique contemporain, a conceptualisé cinq types de liberté, parmi lesquelles figure la liberté d'autodétermination[1477]. Celle-ci serait « le pouvoir ou la capacité à agir de sa propre volonté libre, au sens d'une volonté (caractères, motifs et

---

[1473] V. not. P. Lewis, « 'Fiction is outperforming reality' : how YouTube's algorithm distorts truth », *The Guardian* 2 févr. 2018 ; M. Fisher et A. Taub, « How YouTube radicalized Brazil », *The New York Times* 11 août 2019. Une récente étude montre que l'algorithme de YouTube a tendance à diriger l'utilisateur vers du contenu de plus en plus radical, v. M. Ledwich et A. Zaitsev, « Algorithmic extremism : examining YouTube's rabbit hole of radicalization », *First Monday* 25 févr. 2020, § 5.

[1474] M. Fisher et A. Taub, « How YouTube radicalized Brazil », *The New York Times* 11 août 2019.

[1475] P. Malaurie et L. Aynès, *Droit des personnes. La protection des mineurs et des majeurs*, 8e éd., LGDJ, 2015, nº 312, p. 151 s.

[1476] V. not. CEDH, 29 avr. 2002, *Pretty* c. *Royaume-Uni*, nº 2346/02, § 62 ; CEDH, 17 févr. 2005, *K.A. et A.D.* c. *Belgique*, nº 42758/98 et nº 45558/99, § 83. Pour une analyse de ces jurisprudences, v. F. Sudre (dir.), *Droit européen et international des droits de l'homme,* 14e éd., PUF, 2019, nos 490 s., p. 741 s. Sur le domaine de l'autonomie personnelle, v. M. Fabre-Magnan, « Le domaine de l'autonomie personnelle. Indisponibilité du corps humain et justice sociale », *D.* 2008, p. 31.

[1477] K. Appourchaux, « Neurosciences et techniques de redirection de l'attention : redéfinir le libre arbitre en termes d'apprentissage de la maîtrise de nos capacités attentionnelles », *Psychiatrie, Sciences humaines, Neurosciences* 2013, vol. 11, p. 43, spéc. p. 45.

buts) créée par soi-même ; une volonté que l'on est soi-même, jusqu'à un certain degré, ultimement responsable d'avoir formée »[1478]. Selon cette conception, une personne ne peut être libre que si elle a contribué à forger elle-même son propre caractère et donc, sa propre volonté[1479]. Le concept de liberté d'autodétermination est donc *nécessaire* à la réalisation de celui d'autonomie personnelle : sans liberté dans la formation de la volonté, celle-ci ne peut s'exprimer librement. En effet, c'est seulement parce que la personne est libre au stade de la formation de sa volonté et de ses choix qu'elle est libre au moment de leur réalisation.

395. Concept italien de *libertà di autodeterminazione*. En apparence, ce concept fait écho à celui de *libertà di autodeterminazione* connu du droit italien[1480]. Les contours de celui-ci ont été esquissés à l'occasion d'une décision de la Cour constitutionnelle italienne relative à l'interdiction absolue d'accéder à la fécondation *in vitro* en cas de stérilité ou d'infertilité médicalement prouvée[1481]. La Cour constitutionnelle avait affirmé que le choix des demandeurs à l'instance de devenir parents et de fonder une famille avec enfants relevait de leur *libertà di autodeterminazione* et concernait la sphère de leur vie privée et familiale, protégée en tant que telle par les articles 2, 3 et 31 de la Constitution italienne[1482]. En reconnaissant aux personnes un tel pouvoir de choix, la *libertà di autodeterminazione* du droit italien protège la volonté en tant que telle, et non le processus de formation de celle-ci. En réalité, le concept italien se rapproche plutôt de celui d'autonomie personnelle développé par la jurisprudence de la CEDH[1483]. Bien que ces concepts soient pertinents, ils ne permettent pas d'étendre la protection de la personne au stade de la formation de sa volonté.

396. La liberté d'autodétermination en droit. La transposition de la conception philosophique de la liberté d'autodétermination en droit permettrait de reconnaître une

---

[1478] R. Kane, *A contemporary introduction to free will,* Oxford University Press, 2005, p. 172.
[1479] K. Appourchaux, « Neurosciences et techniques de redirection de l'attention : redéfinir le libre arbitre en termes d'apprentissage de la maîtrise de nos capacités attentionnelles », *Psychiatrie, Sciences humaines, Neurosciences* 2013, vol. 11, p. 43, spéc. p. 46.
[1480] Au sens littéral, l'expression se traduit par « liberté d'autodétermination ».
[1481] Cour constitutionnelle italienne, 9 avr. 2014, n° 162/2014.
[1482] Cour constitutionnelle italienne, 9 avr. 2014, n° 162/2014, § 4.1.
[1483] CEDH, 29 avr. 2002, *Pretty* c. *Royaume-Uni*, n° 2346/02, § 61. D'ailleurs, la CEDH s'est prononcée sur les contours de cette notion de droit italien dans une décision de 2015. Il était question de l'éventuelle reconnaissance du droit de disposer d'un embryon humain *in vitro* en tant que composante du droit au respect de la vie privée de la femme dont les gamètes ont été utilisées pour la conception de l'embryon, v. CEDH, 27 août 2015, *Parillo* c. *Italie*, n° 46470/11, § 149 s.

protection à la formation de la volonté des personnes. Cette liberté d'autodétermination serait donc une sorte de prérequis à l'effectivité de l'autonomie individuelle. En effet, elle permet à la personne de former librement sa volonté, sans être soumise à des influences extérieures prolongées, afin de mener sa vie selon sa propre volonté. Bien sûr, il n'est pas question de remettre en cause le besoin de toute personne d'entretenir avec les autres des relations sociales qui peuvent avoir une influence sur les choix personnels. Il s'agit plutôt d'encadrer les traitements de données qui, sur le long terme, nous influencent. La liberté d'autodétermination est donc centrale, indispensable même, à la substance de l'autonomie personnelle. Sans liberté d'autodétermination, la personne ne peut mener sa vie comme elle l'entend, puisque sa volonté est orientée par des intérêts extérieurs dont elle n'a pas toujours conscience. L'influence ou la manipulation au stade de la formation de la volonté aboutit nécessairement à son entrave au stade de son expression et au rétrécissement de l'autonomie personnelle. D'ailleurs, le droit des contrats protège non seulement l'expression de volonté, mais aussi la réflexion qui a permis d'arriver à cette volonté[1484]. Si une personne a été trompée par les manœuvres de son cocontractant, il n'y a point de consentement valable et le contrat est déclaré nul[1485].

Le concept de liberté d'autodétermination, entendu comme le pouvoir d'une personne de former sa volonté de manière autonome, participe donc à l'autonomie personnelle.

397. Le droit des données personnelles et la liberté d'autodétermination. Le droit des données personnelles apporte quelques garanties pour encadrer les risques que les technologies font courir à la liberté d'autodétermination[1486]. Par exemple, l'obligation d'information sur les finalités pour lesquelles les données sont traitées[1487] ou les obligations de transparence sur les traitements effectués[1488] contribuent indéniablement à une meilleure connaissance des traitements de données et, en théorie, à une meilleure

[1484] F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, nº 147, p. 183.
[1485] Le parallèle avec le droit des contrats trouve sa limite dans plusieurs encadrements des vices du consentement, notamment le « bon dol » ou l'erreur non déterminante.
[1486] Pour certains auteurs, cela serait même la raison des régimes de protection des données, v. Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », in *État de droit et virtualité*, dir. K. Benyekhlef et P. Trudel, Thémis, 2009, p. 157 s., spéc. p. 207.
[1487] Art. 13 § 1 c) et 14 § 1 c) du règlement UE nº 2016/679.
[1488] L'article 12 du règlement UE nº 2016/679 pose le principe de transparence des informations.

compréhension de leurs effets. La personne concernée peut plus facilement identifier les influences auxquelles elle pourrait être soumise. Pour autant, comme souvent en droit des données à caractère personnel, la mise en œuvre effective de ces principes est souvent lacunaire.

Pour rendre effective la liberté d'autodétermination ainsi que le pouvoir de contrôle des personnes sur leurs informations, certains principes du droit des données doivent être renforcés et leur mise en œuvre doit être substantiellement améliorée.

398. Conclusion de chapitre. L'évolution du droit des données personnelles montre un mouvement de responsabilisation des organismes. Au régime déclaratif s'est substitué un régime de responsabilité, accompagné d'un lourd arsenal répressif. Cette évolution tend à rapprocher le droit des données personnelles du droit au respect de la vie privée. Ce rapprochement ne doit toutefois pas masquer que le droit des données à caractère personnel reste un ensemble normatif globalement favorable aux traitements. Ces derniers peuvent être justifiés par une grande variété d'intérêts extérieurs à la personne concernée. En réalité, la protection des personnes apparaît comme l'un des multiples intérêts pris en considération dans cette matière. Même lorsque la volonté de la personne est mise en avant, des contournements restent possibles. Pour les éviter et garantir une protection de la personne conforme à la volonté du législateur, il est impératif d'aller au bout de la logique législative et de reconnaître l'existence d'un contrat spécial au traitement de données à caractère personnel. Ce contrat présente des atouts importants puisqu'il apporte des protections supplémentaires.

Le droit des données à caractère personnel doit donc s'adapter perpétuellement afin de garantir une protection réelle et effective des personnes. Il doit répondre aux nouvelles formes d'atteinte aux personnes permises par les traitements de données. À ce titre, les risques d'atteinte liés à la société de surveillance sont couplés à ceux liés à la société de manipulation. Ces risques doivent être mieux encadrés. Un tel encadrement est crucial pour garantir la liberté d'autodétermination, c'est-à-dire le pouvoir d'une personne de former sa volonté de manière autonome. Pour donner aux personnes un véritable contrôle à l'égard de leurs données, il convient d'adapter certains des principes de la matière.

Chapitre II – Droit prospectif : une protection renforcée des personnes par le droit des données à caractère personnel

399. Un équilibre entre plusieurs intérêts. Le droit des données personnelles repose sur un délicat équilibre entre protection des personnes et permission des traitements[1489]. Le caractère hybride de la protection des personnes, fondée sur des prérogatives embrassant à la fois le contrôle et l'autonomie individuelle, complexifie encore davantage la recherche de cet équilibre. La majorité des auteurs reconnaissent la pertinence de la plupart des principes du droit des données personnelles. Le plus souvent, ces principes réussissent, au moins en théorie, à protéger les personnes à l'égard des traitements de leurs données. Pour autant, il est permis de se demander si certaines règles n'auraient pas tendance à favoriser les traitements au détriment de la protection des personnes. Si tel était le cas, comment ces règles pourraient-elles être ajustées afin de rétablir l'équilibre entre ces deux intérêts ? Les quatre décennies qui nous séparent de l'adoption des premières règles du droit des données personnelles offrent un recul suffisant pour proposer certaines évolutions.

400. Une adaptation nécessaire. Pour Monsieur Samir Merabet, le meilleur moyen d'assurer une protection de la vie privée efficace face aux excès des traitements de données consiste à *limiter* les données collectées[1490]. En apparence, le droit des données à caractère personnel est relativement bien équipé pour mettre en œuvre cet objectif. Par exemple, le principe de minimisation ou l'encadrement des partages de données avec des tiers s'inscrivent précisément dans ce but. Pour autant, l'analyse de ces principes montre qu'ils sont, en réalité, relativement accommodants pour les responsables du traitement. Les développements technologiques de ces dernières décennies sont les meilleurs témoins de cette souplesse.

Bien entendu, la protection des personnes ne se limite pas aux données collectées : elle doit absolument s'étendre aux effets des traitements effectués grâce à ces données. Dans cette perspective, les règles encadrant les décisions prises sur le fondement de traitements de données personnelles apparaissent essentielles, et leur

[1489] Sur ces développements, v. *supra*, n° 297.
[1490] S. Merabet, *Vers un droit de l'intelligence artificielle,* th. Aix-Marseille, 2018, Dalloz, n° 245, p. 235.

adaptation pourrait permettre de protéger effectivement la liberté d'autodétermination. Enfin, l'exercice de certains droits des personnes peut se révéler problématique, notamment pour la liberté d'information. Les développements récents du droit à l'oubli illustrent ces risques.

Si la plupart des auteurs s'accordent sur la pertinence des principes du droit des données à caractère personnel, il apparaît que des améliorations pour certains d'entre eux sont possibles. Tantôt ce sont les pouvoirs reconnus aux personnes concernées qui présentent des risques pour la protection d'ensemble des personnes, tantôt ce sont les principes applicables aux responsables du traitement qui leur permettent d'empiéter sur la protection des personnes. Comment ces principes doivent-ils évoluer pour garantir une meilleure protection des personnes ?

401. Plan. Pour garantir une protection renforcée des personnes, certains pouvoirs doivent être encadrés (Section I), tandis que certains principes doivent être consolidés (Section II).

SECTION I – ENCADRER DES POUVOIRS

402. Des pouvoirs. Dans le langage courant, le terme pouvoir renvoie à l'idée de maîtrise, ou à la capacité de faire quelque chose[1491]. Dans le langage juridique, il est entendu de manière plus restrictive puisqu'il s'agit de la maîtrise de fait, la force, ou la puissance[1492]. C'est plutôt dans une acception large que la notion de pouvoir doit ici être entendue. Elle vise la capacité des personnes concernées ou des organismes à faire quelque chose. Le droit des données à caractère personnel leur reconnaît des pouvoirs de diverses natures. Par exemple, les personnes concernées se sont vues reconnaître de nouveaux droits à l'égard de leurs données[1493]. Les organismes peuvent quant à eux mettre en œuvre les traitements de données. Parmi ces divers pouvoirs, seuls certains ont tendance à diminuer l'effectivité de la protection des personnes.

403. Encadrer certains pouvoirs. En apparence, rien ne semble rapprocher le droit à l'oubli de l'accès aux données par des tiers. Pourtant, l'un comme l'autre doivent être

[1491] *Dictionnaire de l'Académie française*, 9e éd., *Vo* « Pouvoir », sens II,1.
[1492] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vo* « Pouvoir », sens 1.
[1493] Sur le renforcement des droits des personnes par le règlement européen, N. Martial-Braz, « Le renforcement des droits de la personne concernée », *Dalloz IP/IT* 2017, p. 253.

encadrés pour garantir une meilleure protection des personnes. Le droit à l'oubli a récemment fait l'objet de développements, sans que les éventuels effets négatifs de ce droit n'aient été particulièrement anticipés. Quant au second, il est rarement évoqué dans l'étude des règles du droit des données à caractère personnel, pourtant il est la source d'importantes atteintes aux personnes.

404. Plan. L'étude de l'encadrement du droit à l'oubli (§ I) sera suivie par celle des accès aux données personnelles par des tiers (§ II).

§ I. Le droit à l'oubli

405. Plan. Avant d'être juridique, la question de l'oubli est sociale. La tension entre le besoin d'oubli et celui de mémoire cache en réalité des choix de société. Une succincte étude historique de l'oubli montre l'importance de la mémoire pour les sociétés humaines ainsi que la place réduite qu'il a longtemps occupée (A). Les évolutions technologiques questionnent le rapport de la société à la mémoire, dès lors que le numérique donne l'impression d'une conservation des informations infinie[1494]. Devant cet abîme d'informations accessibles à tous et sans limite de temps, les individus ont revendiqué la reconnaissance d'un droit à l'oubli. Le droit des données à caractère personnel a progressivement accueilli cette revendication (B). Cette consécration n'est-elle pas le témoin d'une approche individualiste de l'accès à l'information au détriment d'un éventuel intérêt supérieur de la société ? Une proposition d'encadrement du droit à l'oubli semble nécessaire pour mieux prendre en considération les différents intérêts en présence (C).

A. La place initialement limitée de l'oubli dans le droit

406. Le temps et le besoin d'histoire. Le temps a cette capacité d'engendrer, dans la mémoire humaine, l'oubli. Comme le remarquaient justement Messieurs Philippe Malaurie et Laurent Aynès, « le temps, en s'écoulant, efface les évènements »[1495]. Ce qui n'a pas été consigné sera progressivement érodé et le mouvement des saisons efface la mémoire des évènements. Pour autant, les sociétés humaines ont toujours eu besoin

[1494] Sur les difficultés de préserver les archives dans le monde numérique, M. Quénet, « Quel avenir pour les archives de France ? Rapport au premier ministre », La Documentation française, 2011, p. 39 s.
[1495] P. Malaurie et L. Aynès, *Cours de droit Civil,* t. 2, *Les Personnes, les incapacités*, 5e éd., Cujas, 1999, no 318.

de se commémorer, notamment pour prendre la juste mesure de ce qu'il ne faut pas reproduire puisque l'histoire « enseigne sur ce qui a été méconnu d'essentiel à l'élévation de l'homme et permet, grâce au souvenir de ce qui a pu être grand et qui s'est corrompu, d'ajuster le présent à ce que la société se représente comme idéal pour le futur »[1496]. Les constituants avaient ainsi proclamé, dans la Déclaration des droits de l'homme et du citoyen de 1789, que « l'ignorance, l'oubli ou le mépris des droits de l'homme sont les seules causes des malheurs publics et de la corruption des gouvernements »[1497]. En considérant que l'oubli peut conduire aux malheurs publics, les constituants affirmaient implicitement que l'analyse du passé est nécessaire à la construction d'un avenir meilleur. C'est la raison pour laquelle toutes les sociétés ont organisé des formes de conservation de leur histoire ou de leurs traditions : les pharaons édifiaient d'imposants temples symbolisant leur puissance par-delà leur vie ; les enfants sont baptisés pour que leur existence, à l'égard du Seigneur, soit éternelle ; les passeurs d'histoires égrènent les récits de certaines tribus pour transmettre leur passé ; les cimetières et les monuments aux morts sont construits pour engager les individus à se recueillir auprès de ceux qui sont partis. Historiquement, seuls les ennemis publics étaient exposés à la *damnatio memoriæ* et donc condamnés à l'oubli[1498].

Au Moyen Âge, le développement des bibliothèques et des archives ecclésiastiques institutionnalise la mise en place de mécanismes pour favoriser la mémoire[1499]. Comme le notait déjà René de Chateaubriand, « sans la mémoire que serions-nous ? Notre existence se réduirait aux moments successifs d'un présent qui s'écoule sans cesse ; il n'y aurait plus de passé, ô misère de nous ! »[1500]. La Révolution renforce encore la conservation de documents en consacrant la naissance des archives publiques, c'est-à-dire la mission d'intérêt général consistant à conserver certains documents sur de très longues périodes de temps, dans le but précis de ne pas oublier[1501]. Cette conservation, organisée et méticuleusement mise en œuvre, offre à la société le pouvoir de s'informer sur le passé. Pour éviter un encombrement inutile des

---

[1496] C. Charrière-Bournazel, « L'oubli, l'histoire et le droit », colloque *Parole, tradition, transmission* de l'association AMA, Casablanca, 24 sept. 2005.
[1497] Préambule de la Déclaration des droits de l'homme et du citoyen.
[1498] J.-M. Bruguière, « Le "droit à" l'oubli numérique, un droit à oublier », *D.* 2014, p. 299.
[1499] P. Chastang, « Moyen Âge : une révolution de l'écrit », *L'histoire* 2019, n° 463, p. 38.
[1500] R. de Chateaubriand, *Mémoires d'outre-tombe*, t. 1, Garnier, 1910, p. 78.
[1501] Le Vocabulaire juridique de l'Association Henri Capitant définit les archives comme l'« ensemble des documents y compris les données quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité », G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vo* « Archives », sens 1.

archives, les services implémentent une collecte sélective et raisonnée des documents à l'expiration des délais de leur utilité administrative ou personnelle[1502]. Parallèlement à cette mise en mémoire, se sont renforcées des formes juridiques d'oubli, fondées sur l'objectif de paix et de tranquillité sociales[1503].

407. Des reconnaissances juridiques de l'oubli. Le droit connaît des mécanismes pour « effacer » certains évènements de la chronologie juridique[1504]. Par exemple, en droit pénal, l'amnistie ou la prescription permettent respectivement d'ôter rétroactivement à certains faits leur caractère délictueux[1505] et de considérer que, passé un certain délai, la société oublierait une infraction en admettant qu'elle ne peut plus être poursuivie[1506]. La prescription serait ainsi fondée sur « la grande loi de l'oubli »[1507].

Toutefois, depuis quelques décennies, des phénomènes signalent le recul de l'oubli en droit, matérialisé notamment par le déclin de la prescription[1508]. Les auteurs s'accordent pour reconnaître une indéniable hostilité de la jurisprudence française à l'égard de celle-ci, redoublant ainsi d'efforts pour faire reculer son point de départ et multiplier les hypothèses d'interruption ou de suspension de son délai[1509]. Le législateur participe également à ce recul en rallongeant les délais de la prescription[1510]. En opposition avec cette dynamique juridique et sociale selon laquelle la prescription – et par là même l'oubli – serait contraire à l'intérêt général, le droit des données à caractère personnel réserve, quant à lui, une place de plus en plus importante à l'oubli.

[1502] Ministère de la culture et de la communication, « Préconisations relatives au tri et à la conservation des archives produites par les communes et structures intercommunales dans leurs domaines d'activité spécifiques », 22 sept. 2014.
[1503] B. Bouloc, *Procédure pénale,* 27e éd., Dalloz, 2019, nº 232, p. 194.
[1504] Selon une opinion doctrinale, l'oubli « semble inconciliable, dans son essence même, avec l'approche juridique ». L'affirmation est immédiatement pondérée puisque l'auteur considère que « si le droit ne peut lui-même connaître l'oubli, rien n'interdit, en revanche, d'utiliser un dispositif juridique pour garantir au citoyen le droit de jouir de l'oubli », v. R. Letteron, « Le droit à l'oubli », *Revue du droit public et de la science politique en France et à l'étranger* 1996, t. 112, p. 386.
[1505] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vº* « Amnistie ».
[1506] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vº* « Prescription », sens 2.
[1507] Pour une analyse de cette notion comme fondement principal de la prescription, v. J. Danet, S. Grunvald, M. Harzog-Evans et Y. Le Gall, *Prescription, amnistie et grâce en France*, Rapport final, mars 2006, p. 118 s.
[1508] Pour une critique de ce recul v. A. Chemin, « "Une société sans oubli est une société tyrannique" : pourquoi le principe juridique de la prescription est remis en cause », *Le Monde* 10 janv. 2020
[1509] Pour un exposé des arguments échangés sur les évolutions de la prescription, v. J. Pradel, *Procédure pénale,* 20e éd., Cujas, 2019, nº 253, p. 254 s. ; M.-L. Rassat, *Traité de procédure pénale*, PUF, 2001, nº 297, p. 476 s.
[1510] V. par ex., loi nº 2017-242 du 27 févr. 2017 portant réforme de la prescription en matière pénale, *JORF* 28 févr. 2017, nº 0050, texte 2.

B. Le développement du droit à l'oubli

408. Les prémices du « droit à » l'oubli. À l'oubli d'ordre public imposé par l'autorité de l'État dans l'intérêt général s'ajoute un oubli relatif dans un but de protection de l'individu, censé être contrôlé par le juge[1511]. La première trace de celle-ci provient d'un jugement du tribunal de la Seine de 1965[1512] se prononçant sur la demande en réparation du préjudice subi par la diffusion d'un film rappelant au public une période lointaine et dramatique de la vie privée d'une ancienne maîtresse du tristement célèbre tueur en série Henri Désiré Landru[1513]. Le tribunal évoquait « la prescription du silence » en affirmant pourtant que celle-ci ne « saurait jouer lorsqu'il s'agit d'un procès aussi retentissant que l'affaire Landru »[1514]. Ainsi, même si le tribunal refusait de reconnaître à l'ancienne maîtresse le bénéfice de cette prescription du silence, il reconnaissait implicitement cette possibilité. Il ouvrait donc la voie à la reconnaissance d'une nouvelle forme juridique d'oubli : celle liée à la possibilité pour une personne d'effacer des informations la concernant lorsqu'un certain temps s'est écoulé[1515]. Avec ce nouveau droit, il n'était plus question d'absoudre le passé (comme le fait l'amnistie) ou de reconnaître l'absence d'effet de certains actes après l'écoulement d'un délai (comme c'est le cas pour la prescription), mais plutôt de restreindre la possibilité pour le public de prendre connaissance de certains faits du passé sans, pour autant, que leur véracité ne soit contestée. Ce jugement acte l'émergence d'un droit à l'oubli, fondé sur le droit de contrôle à l'égard d'informations personnelles.

Ce pouvoir a continué de progresser en France avec l'adoption de la loi du 24 juin 1970 concernant la centralisation de la documentation relative à la circulation routière qui prévoyait pour les personnes concernées la possibilité de faire rectifier, voire radier, certains renseignements relatifs à leurs permis de conduire[1516]. Les

---

[1511] R. Letteron, « Le droit à l'oubli », *Revue du droit public et de la science politique en France et à l'étranger* 1996, t. 112, p. 406.
[1512] Trib. Seine, 4 oct. 1965, *JCP* 1966, II, p. 14482.
[1513] Henri Désiré Landru a été condamné pour le meurtre de dix femmes et du fils de l'une d'entre elles. Il avait pour habitude de séduire des dames par petites annonces, leur promettre le mariage (il aurait eu environ 283 fiancées), leur demander leurs économies, les emmener en train dans sa maison de campagne, puis sur place, les faire disparaître, v. S. Duncan, « L'affaire Landru », *France inter* 10 nov. 2019.
[1514] Le tribunal remarquait la conformité de l'œuvre, « non seulement aux chroniques judiciaires, mais aux mémoires publiés par la demanderesse elle-même, qui aurait tenté d'en publier d'autres dans le court de l'année 1963 », Trib. Seine, 4 oct. 1965, *JCP* 1966, II, p. 14482.
[1515] D'ailleurs, Gérard Lyon-Caen, après avoir évoqué les différents fondements juridiques invoqués par la demanderesse, se demandait si « le droit à l'oubli n'eut-il pas été un plus exact fondement ? », G. Lyon-Caen, obs. ss Trib. Seine, 4 oct. 1965, *JCP* 1966, II, p. 14482.
[1516] Art. 7 et 8 de la loi nº 70-539 du 24 juin 1970 concernant la centralisation de la documentation relative à la circulation routière, *JORF* 25 juin 1970, nº 146, p. 65.

articles 9 du code civil et 8 de la CESDH ont également été invoqués pour demander le retrait d'informations personnelles considérées comme obsolètes[1517]. Mais c'est sur le fondement de la loi du 6 janvier 1978 que les personnes ont trouvé le terreau le plus fertile pour faire prospérer leur droit à l'oubli[1518].

409. Le recours au droit d'accès pour faire effacer des données. L'évolution des technologies, notamment celles liées à la mémorisation, au stockage, à l'organisation et à l'accès des données, a redéfini les contours de la mémoire. Ces technologies ont tendance à enrayer le mécanisme d'effacement progressif des souvenirs. Face au sentiment que « Internet n'oublie rien », les personnes se sont inquiétées de voir réapparaître, des années plus tard, des informations les concernant qu'elles pensaient perdues dans les abimes de l'oubli[1519]. Comme le remarquait Jean Foyer, « l'ordinateur a une mémoire qui, à la différence de la mémoire des hommes, n'a pas la faculté d'oublier. Il oublie que ce qu'on efface en lui »[1520].

À ces modalités renouvelées de gestion de l'information s'est ajoutée la démocratisation de l'utilisation d'Internet, avec une propension croissante des individus à partager des informations sur eux-mêmes. Ces facteurs ont encouragé les personnes à revendiquer un plus grand pouvoir de contrôle sur leurs données[1521]. Elles ont ainsi invoqué devant les juridictions la reconnaissance d'un droit à l'oubli sur le fondement du droit d'accès aux données[1522]. En effet, le droit d'accès offrait à la personne concernée le pouvoir d'exiger que « soient rectifiées, complétées, clarifiées, mises à jour ou effacées les informations le concernant qui sont inexactes, incomplètes, équivoques, périmées »[1523]. Ce pouvoir d'exiger du responsable du traitement

---

[1517] A. Marais, « Le droit à l'oubli numérique », in *La communication numérique, un droit, des droits*, dir. B. Teyssié, Éd. Panthéon-Assas, 2012, n^os^ 7 s., spéc. p. 68 s.
[1518] Pour une analyse des sources favorables à ce droit, v. C. Costaz, « Le droit à l'oubli », *Gaz. Pal.* 1995, n° 207, p. 2.
[1519] B. Eins-Hambourg, « Données personnelles. Internet doit-il se souvenir de tout ? », *Courrier International* 18 nov. 2011.
[1520] J. Foyer, 1re séance du mardi 4 oct. 1977, *JORF AN* 5 oct. 1977, n° 79, p. 5782.
[1521] Sur le pouvoir de contrôle des personnes à l'égard de leurs données, v. *supra,* n° 381.
[1522] Le TGI de Paris reconnaissait la légitimité d'une demande de droit à l'oubli dans une décision de 2009 en considérant « que si l'oubli procédait jadis des faiblesses de la mémoire humaine, de sorte qu'il n'y avait pas à consacrer un "droit à l'oubli", la nature y pourvoyant, la société numérique, la libre accessibilité des informations sur Internet, et les capacités sans limites des moteurs de recherche changent considérablement la donne et justifient pleinement qu'un tel droit soit aujourd'hui revendiqué, non comme un privilège qui s'opposerait à la liberté d'information, mais comme un droit humain élémentaire à l'heure de la société de conservation et d'archivage numérique sans limite de toute donnée personnelle et de l'accessibilité immédiate et globalisée à l'information qui caractérisent les technologies contemporaines et la fascinante insouciance qu'elles suscitent », v. TGI Paris, réf., 25 juin 2009, n° 09/55437. Pour un bref exposé historique de la jurisprudence en la matière, A. Debet, « La protection des données personnelles, point de vie du droit privé », *RDP* 2016, n° 1, p. 17.
[1523] Art. 36 de la loi n° 78-17 du 6 janv. 1978. Après la transposition en droit français de la directive CE n° 95/46, c'est l'article 40 de la loi Informatique et libertés qui prévoyait un tel droit.

l'effacement des données « périmées » est rapidement devenu le fondement des demandes de droit à l'oubli. Si le nombre de ces demandes a augmenté[1524], beaucoup d'entre elles n'aboutissaient pas, surtout lorsque la publication était hébergée par des sites se trouvant en dehors de l'Union européenne. Pour pallier cette difficulté, les personnes ont progressivement dirigé leurs recours vers les moteurs de recherche.

410. Les index, outils indispensables dans l'accès à l'information. L'indexation alphabétique est très ancienne puisqu'elle est connue depuis l'Antiquité. Elle réapparaît avec force au Moyen Âge, afin de faciliter l'accès à la vertigineuse documentation produite à cette époque. Elle se développe notamment avec les registres du moine bénédictin Grégoire de Catino vers 1120, pour aider le lecteur à circuler entre les différents volumes de cet immense travail de mise en écriture de l'histoire et du patrimoine de son établissement[1525].

Tout comme le lecteur a recours à l'index pour trouver une référence dans un livre, l'internaute a recours aux moteurs de recherche pour trouver plus facilement une information sur un site Internet. La tâche principale d'un moteur de recherche consiste donc à trouver des sources et documents sur le Web dont le contenu est pertinent pour une requête effectuée par l'utilisateur[1526]. Les moteurs de recherche ont un rôle similaire à celui des index : ils permettent de trouver rapidement l'information requise, sans passer par une lecture cursive du texte.

La numérisation de nos modes de vie a modifié la manière dont les personnes s'informent. Les encyclopédies Universalis trônant sur les étagères du salon ont été remplacées par Wikipédia, accessible librement, rapidement et gratuitement ; le quotidien glissé dans la boîte aux lettres et lu sur le chemin du travail a été remplacé par les applications et les notifications « push » sur mobile. La plupart des personnes naviguent à travers ces ressources grâce à l'aide de leur moteur de recherche favori. Ainsi, lorsque les moteurs de recherche ont été saisis de demandes de suppression de certains liens, de nombreuses interrogations quant aux contours précis de leurs

[1524] En 2013, la CNIL déclarait recevoir environ un millier de plaintes annuellement sur ce sujet (c'est-à-dire qu'environ 20 % des plaintes étaient liées au droit à l'oubli), CNIL, *Rapport d'activité 2013,* La Documentation française, 2014, p. 4 et 16.
[1525] P. Chastang, « Moyen Âge : une révolution de l'écrit », *L'histoire* 2019, nº 463, p. 43.
[1526] B. Amann, « Recherche d'informations sur le Web », in *Encyclopédie de l'informatique et des systèmes d'information*, dir. J. Akoka et I. Comyn-Wattiau, Vuibert, 2006, p. 557.

obligations se sont dessinées. La Cour de justice de l'Union européenne a apporté quelques réponses dans une décision de 2014.

411. La reconnaissance d'un droit au déréférencement par la Cour de justice. La CJUE a été saisie de l'étendue du droit de contrôle des personnes sur leurs données dans le cadre d'un litige opposant Monsieur Mario Costeja González au quotidien *La Vanguardia* et au moteur de recherche Google. Le nom de cet individu figurait dans deux annonces relatives à une adjudication sur saisie immobilière pratiquée en recouvrement de dettes de sécurité sociale et publiées sur ordre du ministère du travail et des affaires sociales. Douze années plus tard, contrarié de voir apparaître ces résultats sur Internet, Monsieur Mario Costeja González a saisi l'autorité espagnole de protection des données de deux demandes. D'une part, il demandait d'ordonner au quotidien de modifier lesdites pages afin que ses données personnelles n'y apparaissent plus ou d'empêcher leur indexation par les moteurs de recherche[1527]. D'autre part, il souhaitait que Google soit contraint de supprimer ou d'occulter ses données personnelles afin qu'elles cessent d'apparaître dans les résultats de recherche et ne figurent plus dans des liens de *La Vanguardia*. Selon Monsieur Mario Costeja González, la saisie immobilière qui avait justifié cette publication avait été réglée depuis plusieurs années, et sa mention était donc dépourvue de toute pertinence.

L'autorité espagnole avait rejeté sa réclamation contre le quotidien, estimant que la publication de ces informations était légalement justifiée[1528]. En revanche, elle avait accueilli favorablement celle visant Google en considérant que le moteur de recherche était soumis aux règles de protection des données, et qu'à ce titre, il lui revenait de retirer des données ou d'interdire l'accès à certaines données « lorsque leur localisation et leur diffusion sont susceptibles de porter atteinte au droit fondamental de protection des données et à la dignité des personnes au sens large, ce qui engloberait la simple volonté de la personne intéressée que ces données ne soient pas connues par des tiers », et cela même lorsque « le maintien de ces informations sur ce site est justifié par une disposition légale »[1529]. Ainsi, la Cour de justice a consacré sans le nommer,

[1527] Parmi les outils permettant d'empêcher le référencement de certaines pages, il existe notamment la possibilité de bloquer l'indexation par le « robots.txt », v. M. Denizon, « Comment empêcher l'indexation d'un site internet ? », *Maxime-Denizon.fr* 25 mars 2015.
[1528] CJUE, 13 mai 2014, *Google Spain SL, Google Inc.* c. *Agencia Española de Protección de Datos, Mario Costeja González,* C-131/12, § 16.
[1529] CJUE, 13 mai 2014, *Google Spain SL, Google Inc.* c. *Agencia Española de Protección de Datos, Mario Costeja González,* C-131/12, § 17.

sur le fondement de la protection des données personnelles, un « droit à l'oubli »[1530]. De manière surprenante, la mise en œuvre de ce droit impose au *moteur de recherche* d'opérer une mise en balance entre l'intérêt et les droits fondamentaux de la personne concernée de voir supprimer ces liens, son intérêt en tant que moteur de recherche et l'intérêt du public à disposer de cette information[1531]. En dépit des critiques exprimées à l'encontre de cet arrêt[1532], ses principes ont été repris par le règlement européen qui a inscrit, dans son article 17, un droit à l'effacement.

412. Le droit à l'effacement (« droit à l'oubli ») dans le règlement européen. Le règlement européen a scellé, dans son article 17, la reconnaissance du droit à l'effacement de données personnelles[1533]. L'article prévoit en effet que la personne « a le droit d'obtenir du responsable du 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 dans les meilleurs délais », lorsque l'un des motifs énumérés par cette disposition s'applique. Six motifs sont successivement présentés, mais seul l'un d'eux (celui relatif aux mineurs) consacre explicitement un droit à l'oubli[1534]. Les cinq autres hypothèses sont de simples déclinaisons des cas de non-conformité rendant l'effacement obligatoire[1535]. En effet, comme le remarque Madame Nathalie Martial-Braz, le droit à l'oubli n'existe que si la personne concernée a le droit

---

[1530] L'apport de cet arrêt est triple : il clarifie le statut des moteurs de recherche en les qualifiant, sans détour, de responsables du traitement de données personnelles ; il affirme que le droit européen s'applique à Google dès lors que les activités de régie publicitaire de la société Google Espagne étaient indissociables de celles de Google Search ; et il reconnaît explicitement un droit au déréférencement et à l'oubli, v. O. Tambou, « Protection des données personnelles : les difficultés de la mise en œuvre du droit européen au déréférencement », *RTD eur.* 2016, p. 249.

[1531] CJUE, 13 mai 2014, *Google Spain SL, Google Inc.* c. *Agencia Española de Protección de Datos, Mario Costeja González,* C-131/12, § 96 s.

[1532] V. not. D. Forest, « Google et le "droit à l'oubli numérique" : genèse et anatomie d'une chimère juridique », *RLDI* 2014, nº 106, p. 76 ; R. Perray et P. Salen, « La Cour de justice, les moteurs de recherche et le droit "à l'oubli numérique" : une fausse innovation, de vraies questions », *RLDI*, 2014, nº 109, p. 35 ; V.-L. Benabou et J. Rochfeld, « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte I : Le moteur, facilitateur d'accès, agrégateur d'informations et responsable de traitement autonome », *D.* 2014, p. 1476 ; N. Martial-Braz et J. Rochfeld, « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte II : le droit à l'oubli numérique, l'éléphant et la vie privée », *D.* 2014, p. 1481 ; L. Marino, « Comment mettre en œuvre le "droit à l'oubli" numérique ? », *D.* 2014, p. 1680 ; E. Netter, « La gestion par les responsables publics de leur réputation en ligne. Réflexions inquiètes sur les déséquilibres du droit au déréférencement », in colloque *La vie privée des responsables publics*, dir. C.-E. Sénac, févr. 2019, Amiens.

[1533] Les guillemets et parenthèses entourant le droit à l'oubli témoignent de la frilosité du législateur dans la reconnaissance d'un droit à l'oubli, v. N. Martial-Braz, « Le renforcement des droits de la personne concernée », *Dalloz IP/IT* 2017, p. 253.

[1534] Pour une étude du droit à l'oubli pour les mineurs, v. O. Foret, « Le droit à l'oubli des mineurs », *Dalloz IP/IT* 2018, p. 350.

[1535] Le premier cas est lié au principe de conservation limitée aux finalités, le deuxième est fondé sur le retrait du consentement, le troisième cas est une application du droit d'opposition, le quatrième cas est en rapport avec à un traitement illicite, et le cinquième cas est lié au respect d'une obligation légale, v. N. Martial-Braz, « Le droit au déréférencement : vraie reconnaissance et faux-semblants ! », *Dalloz IP/IT* 2019, p. 631.

de demander l'effacement de ses données, même lorsque le traitement effectué est licite[1536]. À défaut, point d'oubli, l'effacement est la simple conséquence de l'illicéité du traitement[1537]. Face à la prudence du législateur européen, plusieurs auteurs se sont interrogés sur la portée exacte du droit affirmé par l'article 17 de ce texte[1538].

Dans une série de décisions, la CJUE a mis fin à ces incertitudes puisqu'elle a affirmé, de manière explicite cette fois, l'existence d'un véritable droit à l'oubli sur le fondement du droit des données personnelles[1539]. Pour pouvoir bénéficier de ce droit, il suffit que le traitement des données licitement effectué à l'origine devienne, avec le temps, incompatible avec le droit des données personnelles.

413. Distinguer le droit à l'oubli des autres obligations d'effacement de données. La principale caractéristique de ce droit est qu'il peut s'exercer en dehors de toute illicéité du traitement et que la personne concernée n'a pas à justifier d'un motif légitime ni d'un préjudice pour obtenir l'effacement de ses données[1540]. Il doit donc être distingué des autres obligations liées à l'effacement des données, telles que les limites relatives à la durée de conservation et les cas de retrait du consentement. Le droit à l'oubli reconnaît aux personnes concernées le pouvoir de faire supprimer des informations les concernant en dehors de toute illicéité du traitement. Ainsi, il a tendance à octroyer aux individus le pouvoir de dessiner les contours de la mémoire collective[1541].

[1536] N. Martial-Braz, « Le renforcement des droits de la personne concernée », *Dalloz IP/IT* 2017, p. 253.
[1537] N. Martial-Braz, « Le droit au déréférencement : vraie reconnaissance et faux-semblants ! », *Dalloz IP/IT* 2019, p. 631.
[1538] Sur la difficulté d'interprétation de l'article 17 du règlement européen, v. par ex. M. Boizard, « Le temps, le droit à l'oubli et le droit à l'effacement », *Les cahiers de la justice* 2016, p. 619 ; I. Gheorghe-Bădescu, « Le droit à l'oubli numérique », *RUE* 2017, p. 153.
[1539] Bien que les arrêts aient été rendus sous l'empire du droit antérieur au règlement européen, la Cour a précisé qu'elle prenait en compte l'évolution du droit et que les solutions seraient transposables, v. CJUE, 24 sept. 2019, *Google LLC* c. *Commission nationale de l'informatique et des libertés,* C-507/17, § 46 et CJUE, 24 sept. 2019, *GC, AF, BH, ED* c. *Commission nationale de l'informatique et des libertés,* C-163/17, § 54. Une quinzaine de décisions du Conseil d'État, lequel avait sursoit à statuer, ont été prononcées le 6 décembre 2019, v. CE Sec., 6 déc. 2019, nº 391000, nº 393769, nº 395335, nº 397755, nº 399999, nº 401258, nº 403868, nº 405464, nº 405910, nº 407776, nº 409212, nº 423326 et nº 429154. À l'occasion de la publication de ces décisions, le Conseil d'État a adopté une fiche juridique sur le droit à l'oubli, Conseil d'État, « Droit à l'oubli : le Conseil d'État donne le mode d'emploi », 6 déc. 2019.
[1540] La CJUE précise que la personne n'a pas besoin de démontrer que l'inclusion de l'information en question dans la liste de résultats lui cause un préjudice, v. CJUE, 24 sept. 2019, *Google LLC* c. *Commission nationale de l'informatique et des libertés,* C-507/17, § 45 et CJUE, 24 sept. 2019, *GC, AF, BH, ED* c. *Commission nationale de l'informatique et des libertés,* C-163/17, § 53. Pour certains auteurs, le droit à l'oubli semble être un droit subjectif, v. N. Martial-Braz, « Le renforcement des droits la personne concernée », *Dalloz IP/IT* 2017, p. 253.
[1541] M. Clément-Fontaine, « L'union du droit à la protection des données à caractère personnel et du droit à la vie privée », *Légicom* 2017, nº 59, p. 61, spéc. p. 67.

C. Pour une amélioration du droit à l'oubli

414. Plan. Certains aspects du droit à l'oubli, tel qu'il a été consacré, doivent faire l'objet de critiques (1). Si un tel droit devait perdurer, ses principes devraient être encadrés pour répondre à ces critiques (2).

1. Critiques du droit à l'oubli

415. Les atteintes aux libertés. Pour prévenir les risques d'atteintes aux libertés d'expression et d'information inhérents au droit à l'oubli, le paragraphe 3 de l'article 17 du règlement européen prévoit des circonstances dans lesquelles celui-ci est inopérant. Par exemple, il ne s'applique pas lorsque le traitement est nécessaire « à l'exercice du droit à la liberté d'expression et d'information ». Seules deux libertés sont expressément citées comme limite au droit à l'oubli. *Quid* de la protection des autres libertés face à ce droit, notamment la liberté de pensée ou la liberté d'entreprise[1542] ? En l'absence de référence explicite aux autres libertés protégées par la Charte des droits fondamentaux, celles-ci pourraient-elles prétendre restreindre la mise en œuvre du droit à l'oubli ? La question est délicate parce que le droit à l'oubli est reconnu comme l'une des prérogatives du droit à la protection des données à caractère personnel, lequel est consacré par l'article 8 de la Charte des droits fondamentaux. Ainsi, le droit à l'oubli semble pouvoir limiter l'exercice d'autres libertés, pourtant protégées par la Charte, sans que cette articulation n'ait été particulièrement bien définie par le législateur.

416. Le droit à l'oubli et la liberté d'autodétermination. Le droit à l'oubli est le témoin de la volonté du législateur et des juges de rendre effectif le droit de contrôle des personnes à l'égard de leurs informations personnelles. Pourtant, analyser le droit à l'oubli sous le seul angle de cette prérogative, c'est faire fi de l'aspect social dont les informations sont le vecteur, et cela revient à occulter leur rôle pour la liberté d'opinion et la liberté d'autodétermination. En effet, le droit à l'oubli transforme le droit des données personnelles en droit de (non) utilisation des données. En cela, il se concentre sur un objectif individuel et détourne le régime juridique de son objectif de protection

[1542] Pourtant, la liberté d'entreprise était citée dans les conclusions de Monsieur l'avocat général Niilo Jääskinen, N. Jääskinen, concl. prés. 25 juin 2013, CJUE, 13 mai 2014, *Google Spain SL, Google Inc.* c. *Agencia Española de Protección de Datos, Mario Costeja González,* C-131/12, § 120 s.

des valeurs démocratiques fondamentales que sont l'autonomie individuelle et la délibération démocratique[1543]. En limitant le droit des données personnelles au seul droit de contrôle des personnes à l'égard de leurs données, le droit à l'oubli porte atteinte à la liberté d'information des autres personnes et, par extension, à la liberté de se forger librement sa propre opinion.

Il est classique d'affirmer que le principe de libre circulation des informations rencontre sur son chemin celui de protection des données relatives aux personnes[1544]. Cette rencontre est communément présentée comme conflictuelle : la liberté d'information est opposée à la protection des données personnelles[1545]. Cette opposition frontale s'explique par une approche très empirique : une affaire oppose une personne qui affirme un droit à l'effacement de ses données à un responsable du traitement qui invoque une ou plusieurs libertés. Cette approche est toutefois limitée puisqu'elle oppose un responsable du traitement à la « victime », en minimisant l'effet de l'accès à cette information pour les tiers. Pourtant, un tel accès leur permet de développer leur opinion personnelle sur le sujet. C'est seulement en ayant accès à des informations variées et qui ne font pas l'objet de manipulations que les personnes peuvent développer librement leur opinion[1546]. C'est pourquoi l'interaction entre la protection des données à caractère personnel et les autres libertés ne doit pas être limitée à une opposition entre protection et circulation : ces collisions s'accompagnent également d'un apport réciproque. Puisque la liberté d'information garantit à toute personne le droit d'avoir accès et de diffuser des informations, elle aide les individus à développer librement leur opinion et, par-là, leur personnalité. En permettant de recevoir et de diffuser des informations, la liberté d'information participe, de manière indirecte, au développement libre et autonome de la personnalité et renforce donc la protection de la liberté d'autodétermination et l'épanouissement personnel[1547]. En réduisant les

---

[1543] Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », in *État de droit et virtualité*, dir. K. Benyekhlef et P. Trudel, Thémis, 2009, p. 157 s., spéc. p. 169.
[1544] B. Teyssié, *Droit des personnes*, 21e éd., LexisNexis, 2019, nos 158 s., p. 150 s. ; v. *supra*, no 234.
[1545] Par exemple, dans son rapport au Sénat, Monsieur Alex Türk expliquait que « il y a incontestablement une antinomie entre la protection de la vie privée, des données personnelles et l'exercice large de la liberté d'expression, essentiel dans un État démocratique », A. Türk, « Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », Sénat, no 218, 19 mars 2003, p. 78.
[1546] V. *supra*, no 234.
[1547] CEDH, 7 déc. 1976, *Handyside* c. *Royaume-Uni*, no 5493/72, § 49 ; CEDH, 29 avr. 2002, *Pretty* c. *Royaume-Uni*, no 2346/02, § 61. Sur ce point, v. not. *Rép. civ.* Dalloz, *Vo* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), nos 113 s. et P. Kayser, « Aspects de la protection de la vie privée dans les sociétés industrielles », in *Mélanges G. Marty*, Université des sciences sociales de Toulouse, 1978, p. 725 s., no 3, spéc. p. 727.

informations que les personnes peuvent lire et recevoir, le droit à l'oubli a nécessairement un effet sur leur liberté d'information et donc, à long terme, sur l'autonomie personnelle de l'ensemble des individus. En d'autres termes, le droit à l'oubli tel qu'il a été consacré a tendance à faire primer les intérêts individuels sur ceux de la société.

417. Une mise en balance favorable au droit à l'oubli. À la suite d'une demande de droit à l'oubli, le responsable du traitement doit opérer une mise en balance entre l'intérêt et les droits fondamentaux de la personne concernée de voir supprimer ces liens, l'intérêt du moteur de recherche et l'intérêt du public à disposer de cette information[1548]. Dans cette mise en balance, la nature des données a une influence. Lorsqu'elles sont sensibles, le contrôle de proportionnalité opéré est très strict[1549] ; pour les autres données, ce contrôle est plus souple[1550].

Plusieurs éléments démontrent la prééminence du droit à l'oubli sur les autres intérêts en présence. La CJUE considère que, par principe, les droits à la protection de la vie privée et des données personnelles prévalent « non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, *mais également sur l'intérêt du public à accéder à ladite information* »[1551]. L'affirmation d'un tel principe de supériorité remet en cause la recherche d'un véritable équilibre entre les libertés fondamentales. En ce sens, l'Assemblée parlementaire du Conseil de l'Europe rappelle la nécessité « de trouver la façon de permettre l'exercice équilibré de deux droits fondamentaux, également garantis par la Convention européenne des droits de l'homme : le droit au respect de la vie privée et le droit à la liberté d'expression »[1552]. Elle ajoute d'ailleurs que « ces droits ne sont ni absolus ni hiérarchisés entre eux, étant d'égale valeur »[1553]. En pratique, la Cour de cassation et la CEDH retiennent aussi que le droit au respect dû à la vie privée d'une personne ou à celui de ses données

---

[1548] CJUE, 13 mai 2014, *Google Spain SL, Google Inc.* c. *Agencia Española de Protección de Datos, Mario Costeja González,* C-131/12, § 96 s.
[1549] CJUE, 24 sept. 2019, *GC, AF, BH, ED* c. *Commission nationale de l'informatique et des libertés,* C-163/17, § 68. V. aussi, Conseil d'État, « Droit à l'oubli : le Conseil d'État donne le mode d'emploi », 6 déc. 2019.
[1550] CJUE, 13 mai 2014, *Google Spain SL, Google Inc.* c. *Agencia Española de Protección de Datos, Mario Costeja González,* C-131/12, § 99.
[1551] CJUE, 13 mai 2014, *Google Spain SL, Google Inc.* c. *Agencia Española de Protección de Datos, Mario Costeja González,* C-131/12, § 99. Cette interprétation a été confirmée en 2019, v. CJUE, 24 sept. 2019, *Google LLC* c. *Commission nationale de l'informatique et des libertés,* C-507/17, § 45 et CJUE, 24 sept. 2019, *GC, AF, BH, ED* c. *Commission nationale de l'informatique et des libertés,* C-163/17, § 53.
[1552] Conseil de l'Europe, Assemblée parlementaire, Résolution n° 1165, « Droit au respect de la vie privée », 26 juin 1998, § 10.
[1553] Conseil de l'Europe, Assemblée parlementaire, Résolution n° 1165, « Droit au respect de la vie privée », 26 juin 1998, § 11.

personnelles et le droit à la liberté d'expression ont la même valeur normative et que « il appartient au juge saisi de rechercher un équilibre entre ces droits et, le cas échéant, de privilégier la solution la plus protectrice de l'intérêt le plus légitime »[1554]. À l'inverse, lorsque la CJUE affirme, de manière abstraite, la prévalence d'un intérêt sur les autres, elle enraie la mise en œuvre d'un contrôle de proportionnalité équilibré. La CJUE tempère tout de même ce principe de supériorité en considérant que des raisons particulières, telles que le rôle joué par la personne dans la vie publique, peuvent justifier un refus du déréférencement[1555]. Le moteur de recherche est alors tenu d'effectuer une mise en balance entre le droit du demandeur à voir l'information déréférencée et celui du public à recevoir l'information.

Par ailleurs, le fait que la mise en balance soit opérée une seule fois confirme que celle-ci est favorable au droit à l'oubli. Lorsqu'une page web a été gommée des résultats de recherche attachés au nom d'une personne physique, l'effacement est *définitif*[1556]. Cela peut poser de nombreux problèmes, notamment lorsque le rôle du demandeur dans la vie publique évolue dans le temps[1557]. Par exemple, un banquier d'affaires pourrait solliciter l'effacement et le déréférencement d'informations le concernant avant de devenir conseiller à l'Élysée, puis ministre de l'Économie et enfin président de la République. Le rôle dans la vie publique d'un banquier d'affaires n'est pas comparable à celui d'un ministre ou d'un président de la République. L'absence de réévaluation dans le temps d'un déréférencement peut donc avoir d'importantes conséquences sur le droit du public à l'information.

418. D'importants effets pour la liberté journalistique. Après seulement quelques années d'application, plusieurs exemples démontrent la prédominance du droit à l'oubli sur la liberté d'expression, et le désarroi des journalistes. En effet, le droit consacré à l'article 17 du règlement européen peut non seulement être dirigé vers un moteur de

---

[1554] V. parmi de nombreux exemples, Cass. civ. 1re, 9 juill. 2003, nº 00-20.289, *Bull. civ.* 2003, I, nº 172, p. 134 ; Cass. civ. 1re, 30 sept. 2015, nº 14-16-273, *Bull. civ.* 2016, nº 836 ; CEDH, 7 févr. 2012, *Axel Springer Ag* c. *Allemagne*, nº 39954/08, § 51.

[1555] CJUE, 13 mai 2014, *Google Spain SL, Google Inc.* c. *Agencia Española de Protección de Datos, Mario Costeja González,* C-131/12, § 99.

[1556] E. Netter, « La gestion par les responsables publics de leur réputation en ligne. Réflexions inquiètes sur les déséquilibres du droit au déréférencement », in colloque *La vie privée des responsables publics*, dir. C.-E. Sénac, févr. 2019, Amiens.

[1557] Dans une décision de 2013, le tribunal de grande instance de Paris reconnaît que « l'absence de limite dans le temps » de la demande de suppression d'images, rend la mesure sollicitée trop absolue. Pour pallier ce problème, le tribunal avait ordonné la suppression d'images pour une durée limitée de 5 ans, permettant ainsi une réévaluation de la mesure, v. TGI Paris, 17e ch., 6 nov.2013, nº 11/07970. Ce jugement avait été confirmé en appel, v. CA Paris, 5e ch., 16 juill. 2014, nº 14/05272.

recherche afin qu'il procède au retrait des résultats d'une requête associée aux nom et prénom, mais il peut également être invoqué à l'égard des personnes à l'origine des contenus. Ainsi, les journalistes peuvent être sollicités pour des demandes de retrait de contenu journalistique sur le fondement du droit à l'oubli. C'est souvent le cas d'articles journalistiques de la presse régionale dans lesquels des faits divers locaux sont relatés en incluant les noms des parties impliquées[1558]. Plusieurs journalistes attestent ainsi avoir été obligés d'effacer des pans entiers de leur travail en réponse à ces demandes d'oubli[1559]. Ce droit commence déjà à montrer certains effets inhibiteurs sur la liberté d'expression. C'est surtout dans sa fonction liée au droit au déréférencement que le droit à l'oubli soulève le plus de critiques.

419. Le droit au déréférencement à l'origine d'une censure privée. Le droit au déréférencement a pour effet de confier à un acteur privé le devoir de se placer en *juge* à l'égard des libertés individuelles et d'opérer un contrôle de proportionnalité entre celles-ci[1560]. Le moteur de recherche saisi d'une demande de déréférencement doit en examiner la pertinence et mettre en balance les intérêts en présence afin de savoir s'il va faire, ou non, droit à cette demande[1561]. Comme le remarquent Mesdames Valérie-Laure Benabou et Judith Rochfeld, on assiste donc « *in fine* à une privatisation du jugement de l'information pertinente »[1562]. Une telle censure est inquiétante notamment lorsqu'elle porte sur des articles de presse ou qu'elle permet à des personnes publiques d'obtenir le déréférencement de contenus les concernant. Le nombre de demandes de ce type adressées au moteur de recherche Google est loin d'être négligeable puisque près de 10 % d'entre elles provenaient de personnes publiques et que près de 20 % des

[1558] En Italie et en Angleterre, les pratiques journalistiques ont tendance à révéler les noms des suspects. C'est sans doute ce qui explique qu'environ 30 % de l'ensemble des demandes de retrait adressées à Google sont dirigées contre des articles de presse, T. Bertram *et al.*, « The five years of the right to be forgotten », *CCS'* nov. 2019, Londres.
[1559] A. Satariano et E. Bubola, « One brother stabbed the other. The journalist who wrote about it paid a price », *The New York Times* 23 sept. 2019.
[1560] D'ailleurs, Google a détaillé, dans une lettre au G29, sa procédure de traitement des demandes et notamment la manière dont il fait la balance des intérêts pour décider ou non du déréférencement, Google, « Lettre de Monsieur Peter Fleischer à Madame Isabelle Falque Pierrotin, Présidente du G29 », 31 juill. 2014. Sur une critique de l'absence de contrôle systématique d'une autorité impartiale et indépendante, v. not. M. Clément-Fontaine, « L'union du droit à la protection des données à caractère personnel et du droit à la vie privée », *Légicom* 2017, nº 59, p. 61, spéc. p. 67.
[1561] CJUE, 13 mai 2014, *Google Spain SL, Google Inc.* c. *Agencia Española de Protección de Datos, Mario Costeja González,* C-131/12, § 97 s.
[1562] N. Martial-Braz et J. Rochfeld, « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte II : Le droit à l'oubli numérique, l'éléphant et la vie privée », *D.* 2014, p. 1481, § 8. Plus largement, sur les risques liés à la privatisation de la censure, v. E. Pierrat, « La privatisation de la censure », *Constructif* 2020, nº 56, p. 32 s.

requêtes étaient dirigées contre des sites d'information[1563]. Ces chiffres montrent le nombre important de cas dans lesquels les moteurs de recherche doivent opérer une mise en balance entre deux libertés individuelles, activité qui relève pourtant traditionnellement de la compétence des juges. Un groupement de 80 universitaires s'est inquiété, à juste titre, de l'ampleur du rôle confié à ces acteurs privés[1564].

À ces considérations s'ajoutent également des problèmes de représentation des intérêts en présence. Lorsque le moteur de recherche est saisi d'une demande de déréférencement, il doit prendre en considération son propre intérêt, celui de la supposée victime, celui de l'auteur de la publication litigieuse, et celui de l'intérêt du public à recevoir une telle information[1565]. En instaurant une relation bilatérale entre le moteur de recherche et la présumée victime, la décision exclut *de facto* la défense impartiale des autres intérêts. En effet, l'auteur n'est pas sollicité par le moteur de recherche pour défendre l'accès à sa publication, l'intérêt du public n'est pas représenté par un tiers indépendant, et aucune garantie des droits de la défense n'est prévue[1566]. Si la position du moteur de recherche est une position équivoque, puisqu'il est un tiers tant par rapport à l'auteur de la publication que par rapport à la présumée victime (et également par rapport aux utilisateurs du moteur de recherche), elle ne lui donne pas pour autant les garanties d'impartialité et d'indépendance nécessaires à la réalisation d'un tel contrôle[1567]. Un contrôle indépendant ne sera effectué qu'en cas de conflit d'interprétation entre le moteur de recherche et la supposée victime, puisque c'est seulement dans cette situation qu'un tiers (l'autorité de protection des données ou un juge) peut éventuellement être saisi de l'affaire[1568].

[1563] Pour des analyses détaillées des chiffres publiés par Google liés au déréférencement, v. T. Bertram *et al.*, « The five years of the right to be forgotten », *CCS'* nov. 2019, Londres.

[1564] V. par ex. la lettre ouverte de 80 universitaires demandant la mise en œuvre d'un débat public lié à la mise en œuvre du droit au déréférencement, « Dear Google open letter from 80 academics on "right to be forgotten" », *The Guardian* 14 mai 2015.

[1565] Comme le remarque Madame Olivia Tambou, « La décision de déréférence dépend ainsi de la qualité de la personne requérante, des particularités de l'information dont il est demandé le déréférencement et, enfin, du facteur temps. L'ensemble des indices donnés dans ces trois champs d'interrogation doit servir à l'établissement d'une balance entre différents intérêts, notamment l'intérêt du public au maintien de la diffusion de cette information et la protection de la vie privée et de ses données personnelles », O. Tambou, « Protection des données personnelles : les difficultés de la mise en œuvre du droit européen au déréférencement », *RTD eur.* 2016, p. 249.

[1566] E. Lee, « Recognizing rights in real time : the role of Google in the EU right to be forgotten », *University of California Davis Law Review* 2016, vol. 49, p. 1017 s. [49 U.C. DAVIS L. REV. 1017], spéc. p. 1075.

[1567] Les garanties d'impartialité et d'indépendance sont consubstantielles à l'exercice juridictionnel, v. par ex. *Rép. proc. civ.* Dalloz, *V°* « Magistrat – Le conflit d'intérêt », par L. Balfanti, 2018 (actu 2019), n^os^ 875 s. La doctrine et la jurisprudence ont d'ailleurs toujours considéré qu'il revenait au juge de concilier la protection de la vie privée et les moyens d'information, v. P. Malaurie et L. Aynès, *Cours de droit Civil,* t. 2, *Les Personnes, les incapacités*, 5^e^ éd., Cujas, 1999, n° 313.

[1568] N. Martial-Braz et J. Rochfeld, « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte II : Le droit à l'oubli numérique, l'éléphant et la vie privée », *D.* 2014, p. 1481, § 8.

Le fait qu'une censure privée existe sur un vecteur fondamental de l'accès aux informations altère largement la confiance que les personnes peuvent avoir dans l'indexation, et place les intérêts particuliers devant ceux du groupe. Cette censure a d'importants effets sur l'accès aux informations puisque le moteur de recherche « facilite sensiblement l'accessibilité de ces informations à tout internaute effectuant une recherche »[1569]. À tout le moins, il conviendrait d'imposer aux moteurs de recherche déréférençant des liens une obligation de transparence[1570]. Aujourd'hui, seuls deux moteurs de recherche mettent volontairement à disposition un rapport détaillant le traitement des requêtes de déréférencement[1571].

La position du moteur de recherche est d'autant plus délicate qu'il a également des intérêts dans cette mise en balance[1572].

420. L'absence de prise en compte des conséquences économiques du droit au déréférencement. Lorsque le moteur de recherche est saisi d'une demande en déréférencement, plusieurs éléments influencent son choix de faire droit à cette demande. Une analyse de la situation montre que le moteur de recherche a un intérêt économique à accueillir favorablement les demandes de déréférencement, et ce pour plusieurs raisons. D'une part, si le moteur de recherche souhaite contester le bien-fondé de la demande de déréférencement, parce qu'il pense qu'un autre intérêt est prépondérant sur celui de la présumée victime, il devra engager des frais de procédure et éventuellement des frais de justice pour défendre cette position. Il est donc parfaitement envisageable qu'en cas de doute, le moteur de recherche choisisse de déréférencer les résultats contestés pour éviter un tel contentieux, et cela particulièrement lorsque le moteur de recherche n'est pas une multinationale pouvant financer de tels litiges. D'autre part, puisqu'il n'est pas tenu d'informer l'auteur de la publication litigieuse de son déréférencement (et donc de permettre à celui-ci de

[1569] CJUE, 13 mai 2014, *Google Spain SL, Google Inc.* c. *Agencia Española de Protección de Datos, Mario Costeja González,* C-131/12, § 87.
[1570] V. déjà en ce sens, « Dear Google open letter from 80 academics on "right to be forgotten" », *The Guardian* 14 mai 2015, détaillant les données devant être rendues publiques.
[1571] V. par ex., Google, « Transparence des informations. Demandes de suppression de contenu dans le cadre de la législation européenne sur le respect de la vie privée » ; Microsoft, « Content removal requests report ». Pour autant, tous les moteurs de recherche ne mettent pas ce genre d'informations à disposition du public. Par exemple, le moteur de recherche français Qwant, malgré nos nombreuses demandes, n'a pas mis en place une telle publicité.
[1572] L'intérêt du moteur de recherche est de garantir un accès le plus complet possible aux informations du web.

défendre sa liberté d'expression), il ne craint pas de voir sa décision contestée par l'auteur du contenu litigieux[1573].

421. Une fragmentation dans l'accès à l'information. En reconnaissant qu'une publication peut être maintenue en ligne (car licite), tout en étant désindexée par un moteur de recherche, le droit au déréférencement crée une fragmentation technique de l'accès à l'information[1574]. Cet accès est atrophié pour le grand public puisqu'il n'a pas nécessairement conscience que l'information qu'il cherche a été déréférencée. À l'opposé, les personnes suffisamment averties peuvent mettre en place des techniques de contournement. Puisque l'information est seulement déréférencée, elle n'est pas effacée du site et reste donc accessible sur Internet. La page litigeuse peut être retrouvée sur Internet, voire être référencée par d'autres moteurs de recherche. Par ailleurs, elle reste accessible aux personnes paramétrant leur moteur de recherche sur un pays en dehors de l'Union européenne, puisque le déréférencement ne peut être mondial[1575]. Ce principe a été affirmé par une décision de 2019 dans laquelle la CJUE a rejeté l'interprétation proposée par la CNIL[1576] et a confirmé qu'il n'existe pas, pour l'exploitant d'un moteur de recherche, « d'obligation découlant du droit de l'Union de procéder à un tel déréférencement sur l'ensemble des versions de son moteur »[1577]. Dès lors qu'il est techniquement possible pour une personne ayant quelques compétences techniques d'accéder, depuis le territoire européen, à une extension non européenne du moteur de recherche, l'accès à l'information n'est pas égal pour toutes les personnes. Le droit au déréférencement engendre donc *de facto* un accès différencié à

[1573] Aucune obligation de demande de retrait préalable ne pèse sur la présumée victime et aucune obligation d'information suite au déréférencement ne pèse sur le moteur de recherche. Le paragraphe second de l'article 17 du règlement européen pourrait cependant être interprété comme obligeant le moteur de recherche à faire des efforts raisonnables pour prévenir l'auteur de la publication.

[1574] D'ailleurs, la Cour valide la décision de l'autorité espagnole à l'égard du quotidien *La Vanguardia* en affirmant que la publication par ce journal « était légalement justifiée étant donné qu'elle avait eu lieu sur ordre du ministère du Travail et des Affaires sociales et avait eu pour but de conférer une publicité maximale à la vente publique afin de réunir le plus grand nombre d'enchérisseurs ». Dans son considérant 94, elle prévoit en effet que les pages web « publiées légalement par des tiers et contenant des informations véridiques relatives à la personne » peuvent continuer d'exister, v. CJUE, 13 mai 2014, *Google Spain SL, Google Inc.* c. *Agencia Española de Protección de Datos, Mario Costeja González,* C-131/12, § 94, v. *supra,* nº 411. Personne n'interroge ici la durée de vie de cette donnée et notamment la question de savoir si celle-ci n'est pas périmée (puisque la vente a sans doute eu lieu entre-temps, l'information des enchérisseurs n'est sans doute plus nécessaire), v. CJUE, 13 mai 2014, *Google Spain SL, Google Inc.* c. *Agencia Española de Protección de Datos, Mario Costeja González,* C-131/12, § 16.

[1575] Pour une analyse de cette décision, v. not. T. Douville, « Les variations du droit au déréférencement », *D.* 2020, p. 515, nº 19.

[1576] La CNIL avait enjoint Google d'étendre le bénéfice du déréférencement à « l'ensemble du moteur, quelles que soient les terminaisons utilisées », CNIL, décision nº 2015-047 du 21 mai 2015 mettant en demeure la société Google Inc.

[1577] CJUE, 24 sept. 2019, *Google LLC* c. *Commission nationale de l'informatique et des libertés,* C-507/17, § 64 s.

l'information. Cette obligation a des conséquences sur le droit du public à s'informer[1578] et plus largement sur les libertés individuelles[1579].

Si, historiquement, nous condamnions les ennemis publics à l'oubli, est-il désormais souhaitable de confier le pouvoir de déterminer les contours de l'oubli, et donc de notre mémoire collective, à des intérêts particuliers ? Il faut sans doute espérer que non et proposer un encadrement de ce pouvoir.

2. L'encadrement du droit à l'oubli

422. Restreindre le droit à l'effacement aux publications illicites. En 2013, la CNIL avait conseillé de reconnaître aux personnes le droit de demander le « déréférencement, sans délai à la charge des moteurs de recherche, dès lors que l'internaute a obtenu l'effacement de l'information initiale »[1580]. Adoptant une logique similaire, Madame Astrid Marais avait proposé que « la personne qui entend obtenir le retrait d'information la concernant, doit (…) d'abord agir contre celui qui l'a mise en ligne s'il n'est pas anonyme, et, en cas d'inaction de celui-ci, elle pourra s'adresser à l'hébergeur en lui notifiant l'existence du contenu illicite. Ce dernier sera alors tenu de retirer l'information du site en cause »[1581].

Ces propositions répondent à plusieurs des critiques formulées à l'égard du droit à l'oubli et du droit au déréférencement. D'une part, elles permettent de prendre en compte le droit de l'auteur de la publication, en le plaçant au cœur du dispositif : ce n'est que lorsque celui-ci n'est pas connu ou qu'il ne répond pas que l'hébergeur ou le moteur de recherche doit être sollicité[1582]. D'autre part, ces propositions restreignent le champ d'application des demandes puisque celles-ci ne peuvent porter que sur des

---

[1578] Selon une opinion doctrinale, la Cour a tendance à occulter le rôle essentiel occupé par les moteurs de recherche dans l'accès à l'information et nie l'intérêt général qu'ils servent, v. R. Post, « Tensions entre "droit au débat public" et "droit au déréférencement". Regard d'outre-Atlantique », *RID comp.* 2017, n° 4, p. 821, spéc. p. 844.

[1579] V.-L. Benabou et J. Rochfeld, « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte I : Le moteur, facilitateur d'accès, agrégateur d'informations et responsable de traitement autonome », *D.* 2014, p. 1476, § 7 s.

[1580] CNIL, *Rapport d'activité 2013,* La Documentation française, 2014, p. 4 et 16.

[1581] A. Marais, « Le droit à l'oubli numérique », in *La communication numérique, un droit, des droits*, dir. B. Teyssié, Éd. Panthéon-Assas, 2012, n° 24, spéc. p. 79. Au contraire, pour Mesdames Valérie-Laure Benabou et Judith Rochfeld, « il n'est donc pas souhaitable que l'obligation du moteur soit subordonnée au retrait préalable de l'information auprès de l'éditeur, parce que la responsabilité du traitement lui incombe directement et de façon autonome, pour une activité qui lui est spécifique et entraîne ses propres conséquences », v. V.-L. Benabou et J. Rochfeld, « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte I : Le moteur, facilitateur d'accès, agrégateur d'informations et responsable de traitement autonome », *D.* 2014, p. 1476, § 9.

[1582] Si le retrait est accepté par l'auteur de la publication, celle-ci devrait être effacée et elle ne sera donc plus référencée par les moteurs de recherche.

publications ayant un contenu illicite. Elles surmontent donc l'une des principales difficultés du droit à l'oubli autorisant le retrait de contenus licites à la discrétion de la personne concernée[1583].

Ainsi, lorsque le responsable du traitement ne répond pas (ni favorablement ni défavorablement), la personne devrait pouvoir saisir l'hébergeur ou les moteurs de recherche afin d'obtenir le retrait du contenu contesté. Sur le modèle de ce qui existe en matière de responsabilité des hébergeurs, le moteur de recherche devrait effacer les liens vers du contenu manifestement illicite[1584]. Dans le cas où le moteur de recherche ne se conforme pas à la demande, notamment parce qu'il considère que le contenu n'est pas illicite, sa responsabilité comme responsable du traitement pourrait alors être engagée. Ce mécanisme permettrait de répondre aux besoins de suppression de contenus manifestement illicites, tels que le *revenge porn*[1585], tout en laissant à l'auteur de la publication la possibilité de contester le retrait.

423. Replacer le juge au cœur du dispositif. Si l'informatique et la mise en réseau des ordinateurs ont profondément modifié le rapport des personnes à l'information, la mémoire reste un besoin social. Il est vrai que la mémoire informatique a des capacités incomparables avec la mémoire humaine, qui amènent à repenser la manière dont sont consignés les évènements. Pourtant, il ne semble pas souhaitable que le choix de conserver ou d'effacer des évènements de notre mémoire collective soit dicté par des intérêts particuliers, avec une prépondérance du droit à l'oubli sur les autres libertés.

Les principes qui guidaient la conservation à l'ère pré-numérique devraient continuer de s'appliquer aujourd'hui et les choix de mémoire ou d'oubli devraient être décidés par la société. Seule cette dernière, incarnée par le juge, devrait avoir le pouvoir de se prononcer sur l'oubli réclamé par l'individu. C'est pourquoi, lorsque le retrait est explicitement refusé par l'auteur du contenu, la personne concernée ne devrait pas pouvoir contourner ce refus en obtenant le déréférencement auprès d'un moteur de

---

[1583] En cela, certains auteurs pourraient considérer qu'il ne s'agirait plus d'un droit à l'oubli, v. N. Martial-Braz, « Le droit au déréférencement : vraie reconnaissance et faux-semblants ! », *Dalloz IP/IT* 2019, p. 631.
[1584] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économique numérique, *JORF* 22 juin 2004, n° 0143, texte 2.
[1585] Sur le phénomène du *revenge porn*, c'est-à-dire « la pratique d'une rare inélégance, consistant à mettre en ligne des photographies d'une personne dans son intimité sexuelle, sans qu'elle ait consenti à cette diffusion » (A. Lepage, « L'article 226-2-1 du code pénal. Une nouvelle strate dans la protection pénale de la vie privée », *Dr. pén.* 2017, n° 1, étude 1, § 2), v. Cass. crim., 16 mars 2016, n° 15-82.676, *Bull. crim.* 2016, n° 86, et l'adoption de l'article 226-2-1 du code pénal. Sur ce sujet, v. not. A. Serinet, « L'instauration d'une répression des atteintes à l'intimité sexuelle par la loi pour une République numérique », *D.* 2016, p. 1711. En pratique, les chiffres rendus publics par Google montrent que ces demandes sont peu nombreuses, T. Bertram *et al.*, « The five years of the right to be forgotten », *CCS'* nov. 2019, Londres.

recherche. Si l'auteur de la publication revendique sur celle-ci l'exercice de sa liberté d'expression ou le droit du public à l'information, seul un juge devrait être compétent pour opérer une mise en balance entre ces libertés et éventuellement prononcer une décision d'effacement[1586]. Le juge est le seul à bénéficier des garanties d'indépendance et d'impartialité préservant une prise en considération neutre de tous les intérêts en présence.

Si l'objectif initial du droit à l'oubli était de positionner la personne concernée en maîtresse de ses données, le droit positif a des effets pervers sur les autres libertés. La liberté d'expression est atteinte puisque les journalistes sont contraints d'effacer leur travail. La liberté d'information est également touchée dès lors que les personnes n'ont plus un égal accès à celle-ci. En sus, en retirant du contenu licite sur des principes d'une censure privée, on porte atteinte à la capacité des personnes à se faire leur propre opinion sur un sujet.

Dans un autre domaine, le contrôle de la personne sur ses données devrait être, au contraire, renforcé. Il s'agit de l'accès par des tiers aux données personnelles.

§ II. Les accès par des tiers aux données à caractère personnel

424. Une relation souvent perçue comme bilatérale. Lorsqu'une personne physique confie ses données à un organisme, elle a souvent le sentiment qu'il sera le seul à les traiter. Pourtant, il est courant que l'organisme les communique à de tierces personnes. Comme le remarquait déjà en 2014 le Conseil d'État, « la transmission de données personnelles d'une entité à une autre est porteuse de risques particuliers : dès lors que l'acquéreur des données est une autre entité que celle qui les a initialement collectées auprès de la personne concernée, ses finalités peuvent être différentes. En outre, en dépit des dispositions de l'article 32 de la loi du 6 janvier 1978 sur le droit d'information, la personne concernée n'est que rarement informée de la cession de ses données et ne sait donc plus qui est le responsable de leur traitement. Le risque s'accroît lorsque les transmissions se succèdent »[1587]. De telles communications engendrent donc des risques pour l'effectivité de la protection des personnes. En effet, des tiers peuvent s'approprier des données et effectuer des traitements, sans que la personne concernée

[1586] C'est d'ailleurs ce qui était prévu par la jurisprudence antérieure et approuvé par la doctrine, v. P. Malaurie et L. Aynès, *Cours de droit Civil,* t. 2, *Les Personnes, les incapacités,* 5e éd., Cujas, 1999, no 313.
[1587] Conseil d'État, « Le numérique et les droits fondamentaux », *Rapport Public 2014*, La Documentation française, 2014, p. 183.

en ait nécessairement conscience. Ces communications favorisent l'existence de traitements de données secrets puisqu'une fois que la donnée a été communiquée à un tiers, il est très compliqué pour la personne concernée de savoir l'usage qui en sera fait par ce tiers. Ces communications portent donc atteinte à la relation de confiance existant entre la personne concernée et l'organisme. La question de l'accès à des données par des tiers était l'une des problématiques au cœur du scandale Cambridge Analytica[1588]. L'entreprise avait acheté à un chercheur de l'université de Cambridge une base de données élaborée grâce à une application tierce à la plateforme Facebook. L'application avait permis au chercheur de collecter des données sur les participants, mais surtout sur leurs « amis » Facebook. Les données de pas moins de 50 millions de profils avaient ainsi été collectées. Elles ont ensuite pu être utilisées par l'entreprise Cambridge Analytica pour d'autres finalités, sans que les utilisateurs n'en aient été informés[1589]. Les accès aux données présentent donc d'importants risques pour la protection des personnes.

425. Plan. L'analyse du droit positif montre un encadrement souple des accès aux données par les tiers (A). Pour prévenir les risques liés à ces accès, nous formulerons des propositions juridiques et techniques pour encadrer plus strictement ces accès (B).

A. De lege lata : un encadrement souple

426. Les catégories de tiers pouvant accéder aux données. Le règlement européen distingue trois catégories de tiers pouvant recevoir communication des données, parmi lesquels figurent les sous-traitants, les destinataires et les tiers autorisés.

Le sous-traitant est la personne « qui traite des données pour le compte du responsable du traitement »[1590]. Celui-ci est lié au responsable du traitement par un contrat écrit fixant les conditions dans lesquelles il opère[1591] : il ne peut agir que sur

---

[1588] Wired, « The Cambridge Analytica story, explained. A quick, but thorough overview of the controversy », *Wired* 2018 ; W. Audureau, « Ce qu'il faut savoir sur Cambridge Analytica, la société au cœur du scandale Facebook », *Le Monde* 22 mars 2018.

[1589] Les personnes ont pu être informées de cet éventuel transfert après l'explosion de ce scandale, v. A. Hern, « How to check whether Facebook shared your data with Cambridge Analytica », *The Guardian* 10 avr. 2018. Pour un exposé des techniques utilisées par Cambridge Analytica pour faire de la segmentation d'audience, voir la présentation de Monsieur Alexander Nix PDG de l'entreprise Cambridge Analytica faite à l'occasion du Concordia Annual Summit de New-York en septembre 2016.

[1590] Art. 4 § 9 du règlement UE nº 2016/679.

[1591] L'article 28 § 3 du règlement UE nº 2016/679 fixe les éléments devant être présents dans le contrat de sous-traitance. Sur ces obligations, v. F.-L. Simon et A. Bounedjoum, « RGPD : quelles règles en matière de responsabilité et quels impacts sur les contrats ? », *AJ Contrat* 2018, p. 172.

délégation du responsable du traitement[1592]. En quelque sorte, le sous-traitant opère le traitement au nom et pour le compte du responsable du traitement.

En plus des sous-traitants, les destinataires peuvent également recevoir communication de données personnelles. Le destinataire est « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel »[1593]. Le destinataire se distingue du sous-traitant puisqu'il est un autre responsable du traitement « qui va, à son tour, traiter les données pour des finalités qui lui sont propres »[1594].

Enfin, une troisième catégorie de tiers peut également accéder licitement aux données personnelles collectées par un responsable du traitement : il s'agit des « tiers autorisés ». Ces tiers sont définis comme « 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 »[1595]. En pratique, il s'agit souvent d'autorités légalement habilitées à accéder aux informations, notamment dans le cadre d'enquêtes[1596].

Avec le numérique, les transferts de données sont très rapides et faciles à effectuer pour les organismes, tout en étant très obscurs pour les personnes concernées[1597]. C'est notamment parce que les données sont non rivales que leur communication est rendue si aisée.

427. Les données sont non rivales. À partir des années 1950, des économistes ont développé la théorie de la « rivalité » afin de classifier les biens ou services[1598]. Un

---

[1592] A. Banck, « GDPR et sous-traitance : un nouveau devoir de conseil ? », *Dalloz IP/IT* 2017, p. 36.
[1593] Art. 4 § 9 du règlement UE nº 2016/679.
[1594] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 562, p. 243.
[1595] Art. 4 § 10 du règlement UE nº 2016/679.
[1596] E. Geffrey et A. Guérin-François, « Commentaire sous l'article 4 du règlement UE nº 2016/679 », in *Code de la protection des données personnelles,* Dalloz, 2020.
[1597] Comme le remarquait Madame Juliette Sénéchal, « les données transmises par le client à son contractant seront le plus souvent revendues à des tiers », J. Sénéchal, « La fourniture de données personnelles par le client *via* Internet, un objet contractuel ? », *AJ Contrats d'affaires* 2015, p. 212.
[1598] La notion de rivalité (*rivalry*) ou de soustractabilité (*subtractability*) a été développée par Vincent Ostrom et Elinor Ostrom en 1977 pour distinguer les biens privés des biens publics et pour compléter la notion d'exclusion mise en avant par Paul Samuelson dès 1954, V. Ostrom et E. Ostrom, « Public goods and public choices », in *Alternatives for delivering public services : toward improved performance*, dir. E. Savas, WestviewPress, 1977, p. 7 s. ; P. Samuelson, « The pure theory of public expenditure », *Review of Economics and Statistics* 1954, p. 387 ; R. Musgrave, *The theory of public finance : a study in public economy*, McGraw-Hill, 1959. Sur la classification des biens économiques et une définition du bien public, v. M. Cornu, F. Orsi et J. Rochfeld (dir.), *Dictionnaire des biens communs*, PUF, 2017, *Vº* « Bien public (approche économique) ».

bien ou service est considéré comme *rival* lorsque sa consommation ou son usage rend impossible ou très difficile son utilisation par une autre personne. Il est qualifié de *non rival* si, au contraire, son usage par une personne ne limite pas la possibilité d'utilisation pour les autres. Dans ce cas, plusieurs personnes peuvent donc utiliser simultanément le bien ou service[1599].

Il n'existe pas de doute sur le fait que les données doivent être qualifiées comme non rivales puisque, quel que soit leur nombre, des individus peuvent utiliser une même donnée en parallèle, sans se gêner réciproquement[1600]. À l'inverse, lorsqu'une personne écoute un disque ou regarde un DVD, les tiers sont en situation de rivalité, c'est-à-dire qu'ils ne peuvent pas utiliser simultanément le même disque ou DVD. Par ailleurs, les données ont la particularité de conserver leur valeur malgré l'usage, c'est-à-dire qu'elles ne se consomment pas et ne s'abîment pas en fonction de leur utilisation[1601]. Ces caractéristiques favorisent ainsi la circulation des données et contribuent aux accès par des tiers aux données.

428. Les faibles coûts de circulation des données. À l'absence de caractère rival s'ajoute également le faible coût des opérations effectuées sur les données[1602]. En effet, les coûts liés au stockage et à la transmission d'informations sont de plus en plus réduits et encouragent une vaste collecte de celles-ci[1603]. De plus, les frais techniques liés à la reproduction des données sont très faibles, notamment parce que cette reproduction est automatisée et limitée au coût de la bande passante. Enfin, la baisse constante des coûts

---

[1599] M. Cornu, F. Orsi et J. Rochfeld (dir.), *Dictionnaire des biens communs*, PUF, 2017, *V°* « Bien public (approche économique) ».

[1600] Selon Monsieur Shaun Spencer, « l'information est non rivale, donc un acteur qui collecte de l'information peut la partager avec un nombre illimité de tiers et continuer de l'utiliser pour sa finalité originale », v. S. Spencer, « Reasonable expectations and the erosion of privacy », *San Diego Law Review* 2002, vol. 39, p. 843 s. [39 SAN DIEGO L. REV. 843], spéc. p. 879. V. aussi, R. Hilty, « La privatisation de l'information par la propriété intellectuelle : problème et perspectives », *Revue internationale de droit économique* 2006, vol. 4, p. 353 ; E. Mackaay, « La propriété est-elle en voie d'extinction ? », in *Nouvelles technologies et propriété*, actes du colloque tenu à Montréal, 9 et 10 nov. 1989, E. Mackaay (dir.), Litec, 1991, p. 217 s., spéc. p. 234 ; L. Lessig, *The future of ideas : the fate of the commons in a connected world*, Random House, 2001, p. 21 ; P. Schwartz, « Privacy and democracy in cyberspace », *Vanderbilt Law Review* 1999, vol. 52, p. 1609 s. [52 VAND. L. REV. 1609], spéc. p. 1689 s. ; N. Mallet-Poujol, « Appropriation de l'information : l'éternelle chimère », *D.* 1997, p. 330, n^os^ 6 s. Pour une approche économique, v. R. Cooter et T. Ulen, *Law and economics*, 6^e^ éd., Addison-Wesley, 2012, p. 103.

[1601] E. Mackay, « Les biens informationnels ou le droit de suite dans les idées », in *L'appropriation de l'information*, dir. J.-P. Chamoux, Librairies Techniques, 1986, p. 45 s., spéc. p. 61. Pierre Catala affirmait d'ailleurs que « l'information peut être indéfiniment reproduite en vue de sa conservation ou de sa divulgation », P. Catala, « La "propriété" de l'information », in *Mélanges P. Raynaud*, Dalloz, 1985, p. 97 s., n° 3, spéc. p. 98.

[1602] R. Lacombe, P.-H. Bertin, F. Vauglin et A. Villefosse, « Pour une politique ambitieuse des données publiques. Les données publiques au service de l'innovation et de la transparence. Rapport au ministre de l'Industrie de l'Énergie et l'Économie numérique », École des Ponts ParisTech, 2011, p. 76. V. également, W. Kerner, « A new (intellectual) property right for non-personal data ? An economic analysis », *Gewerblicher Rechtsschutz und Urheberrecht. Internationaler Teil* 2016, vol. 11, p. 9.

[1603] Cela a été théorisé dans les conjectures de Moore, v. *supra*, n° 25.

de stockage encourage une conservation étendue des données. L'absence de rivalité cumulée au faible coût des traitements favorise donc la circulation des données entre les organismes.

429. Les données sont difficilement traçables. Aux faibles coûts de collecte, de stockage et de reproduction des données s'ajoute un élément participant aux transferts de données à des entités tierces : la difficile traçabilité d'une donnée. La traçabilité des données est une expression polysémique. Elle peut être définie d'une part comme la marque laissée par chaque transaction, modification, déplacement, accès… effectués sur une ressource[1604]. Elle est ainsi entendue comme l'un des principes de gouvernance des données, permettant notamment d'avoir la liste chronologique complète des évènements effectués sur une base de données[1605]. Cette liste est souvent générée automatiquement sous forme de *server log* (journal d'évènements), et son analyse permet de vérifier les accès et de s'assurer que seules les personnes autorisées ont pris connaissance des données. D'autre part, la traçabilité des données peut être entendue comme le fait de pouvoir suivre les traces laissées par une donnée lorsqu'elle circule. Par principe, lorsque les données circulent, elles ne laissent pas de traces. Ainsi, lorsque des données sont transférées à des tiers, il n'existe pas d'information technique fournie à la personne concernée par cette transmission, et les tiers qui les reçoivent ne sont pas techniquement obligés d'en établir l'origine[1606]. Cette dernière acception de la notion de traçabilité des données explique la grande circulation des données entre les organismes.

430. La variété des intérêts autorisant l'accès par des tiers aux données. Dans les hypothèses où l'accès aux données personnelles est accordé à un tiers, les intérêts justifiant cet accès sont des plus divers. Ainsi, par exemple, l'accès par le *sous-traitant* est fondé sur la réalisation des finalités du traitement, et le responsable du traitement peut déléguer cette mise en œuvre à un spécialiste. Dans ce cas, l'accès est justifié par la bonne réalisation du traitement et les principes de protection des données sont, en

[1604] Le dictionnaire Larousse définit la traçabilité comme la « possibilité de suivre un objet aux différentes étapes de son acheminement », Larousse, *Dictionnaire de Français, V°* « Traçabilité » ;
[1605] J. Zhang, « Operationalizing data quality through data governance », in *Data governance. Creating value from information assets*, dir. N. Bhansali, CRC Press, 2014, p. 66 s.
[1606] De telles contraintes peuvent être établies par la loi, mais d'un point de vue technique, les données ne laissent pas de trace.

théorie, préservés[1607]. En effet, les obligations contractuelles entourant les communications de données apportent un cadre juridique adéquat et permettent des contrôles tant des responsables du traitement que des sous-traitants[1608].

En revanche, pour les deux autres catégories de tiers (les tiers autorisés et les destinataires), cet accès est fondé sur un intérêt extérieur à la réalisation du traitement initial. Pour les *tiers autorisés*, c'est souvent l'intérêt général qui justifie l'accès aux données. Un tel accès, s'il est encadré par la loi et est exercé de manière ponctuelle et transparente[1609], semble justifié et nécessaire, notamment parce qu'il contribue au bon fonctionnement de la justice[1610].

Pour les *destinataires*, l'accès est justifié par un intérêt particulier, extérieur au traitement réalisé par le responsable du traitement originel. En principe, les destinataires peuvent traiter les données personnelles dont ils ont reçu communication pour une nouvelle finalité, tant que ce traitement n'est pas incompatible avec les finalités initiales du traitement[1611]. En pratique, les responsables du traitement communiquent régulièrement des données à caractère personnel à des tiers, et les règles juridiques entourant ces communications sont finalement peu nombreuses. Cette souplesse s'explique sans doute par la volonté du législateur de permettre la circulation des données. La parcimonie des règles applicables à ces transferts n'a pas empêché l'émergence de destinataires inconnus du grand public et spécialistes du « courtage de données » (dénommées en anglais *data brokers*)[1612].

[1607] Certaines précautions doivent être mises en œuvre afin d'assurer que les traitements de ces données personnelles par le sous-traitant demeurent conformes aux obligations du droit des données personnelles, v. not. A. Cousin, « Réparer le préjudice causé par la violation du RGPD », *Dalloz IP/IT* 2019, p. 553.

[1608] C. Alleaume, « Les données à caractère personnel comme objet de contrat », *AJ Contrat* 2019, p. 319 ; J. Sénéchal, « La fourniture de données personnelles par le client *via* Internet, un objet contractuel ? », *AJ Contrats d'affaires* 2015, p. 212.

[1609] Par exemple, les responsables du traitement pourraient être tenus d'établir un rapport lié à la transparence des informations révélant comment les règles et les actions des autorités et des entreprises affectent la confidentialité, la sécurité et l'accès aux informations en ligne, v. par ex. les rapports « Transparence des informations » de Google.

[1610] En revanche, un accès indifférencié aux données personnelles ne serait pas respectueux du principe de proportionnalité nécessaire dans cette matière. Sur le sujet de la collecte massive des données personnelles auprès d'entreprises privées par le renseignement américain, v. F. Tréguer, « US technology companies and State surveillance in the post-Snowden context : between cooperation and resistance », *CERI* 2018. Sur la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, v. CJUE, 6 oct. 2020, *La Quadrature du Net* c. *Premier ministre*, C-511/18, C-512/18 et C-520/18, § 128 s.

[1611] En vertu de l'article 5 du règlement UE nº 2016/679, les données ne doivent « pas être traitées ultérieurement d'une manière incompatible » avec les finalités déterminées, explicites et légitimes.

[1612] P. Signoret, « J'ai voulu savoir qui avait vendu mes données personnelles et je suis tombée dans un puits sans fond », *Numerama* 25 avr. 2019 ; P. Signoret, « J'ai (enfin) découvert pourquoi des marques inconnues me ciblaient sur Facebook », *Numerama* 12 juin 2019

431. Les entreprises de courtage de données (*data brokers*). Les courtiers de données ont pour objectif d'agréger, d'enrichir, de transformer et de commercialiser des données personnelles. Leurs sources sont variées, et elles récupèrent la majorité de leurs données *à l'insu* des personnes concernées. Aux États-Unis, certaines entreprises revendiquent la détention de données personnelles concernant des centaines de millions d'individus dans le monde[1613]. Ces entreprises sont régulièrement critiquées notamment pour leurs pratiques, leur manque de transparence et les risques liés à la centralisation des données personnelles[1614]. En Europe, bien que les règles de protection soient considérées comme plus restrictives que celles existant aux États-Unis, ces entreprises réussissent à prospérer[1615]. Comme le remarquait la CNIL en 2018, « la technicité de ces systèmes rend ces traitements largement inconnus du grand public, alors même qu'ils touchent une part importante de la population française »[1616]. Le principal problème des entreprises de courtage est qu'elles centralisent un grand nombre de données personnelles, qu'elles traitent souvent pour inférer de nouvelles informations sur les personnes concernées. Elles peuvent ensuite revendre ces données à des tiers, notamment pour qu'ils puissent faire des segmentations du public (par exemple pour les orienter ou leur proposer de la publicité ciblée) ou une évaluation de la personne (par exemple à des fins de recrutement, d'octroi de crédit ou d'assurance)[1617]. L'activité des courtiers de données doit être distinguée de celle des grandes entreprises, telles que Facebook ou Google, qui centralisent d'importantes masses de données sur leurs utilisateurs. Contrairement aux courtiers de données, ces entreprises ne vendent pas l'accès aux données en tant que telles, mais plutôt la possibilité d'afficher des publicités pour certaines catégories d'utilisateurs[1618].

[1613] Par exemple, l'entreprise Axciom revendique la détention de données personnelles concernant 700 millions d'individus dans le monde avec pas moins de 5 000 segments d'informations, v. Axciom, « Annual Report », 2018.

[1614] FTC, « Data Brokers. A call for transparency and accountability », mai 2014 ; U.S. Senate, « A review of the data broker industry : collection, use, and sale of consumer data for marketing purposes », déc. 2013. Dans un domaine similaire (l'évaluation du crédit), la violation de données subie par Equifax en 2017 montre les dangers liés à la centralisation des données, v. I. Vergara, « Piratage de données : Equifax paye 700 millions de dollars pour éteindre les enquêtes », *Le Figaro* 22 juill. 2019.

[1615] Le Conseil d'État regrettait qu'il n'existe pas vraiment d'analyses de fond de l'activité des *data brokers* en Europe, Conseil d'État, « Le numérique et les droits fondamentaux », *Rapport Public 2014*, La Documentation française, 2014, p. 158 s. ; sur cette question voir aussi, C. Koumpli, *Les données personnelles sensibles. Contribution à l'évolution du droit fondamental à la protection des données à caractère personnel*, th. Paris I, 2019, p. 250.

[1616] CNIL, *Rapport d'activité 2018*, La Documentation française, 2019, p. 73. La CNIL a ouvert une enquête sur la société française Criteo, v. not. S. Dumoulin, « Criteo visé par une enquête de la CNIL », *Les Echos* 10 mars 2020.

[1617] Sur les risques de manipulation liés aux traitements de données, v. *supra*, n^os^ 389 s.

[1618] EFF, « Google says it doesn't "sell" your data. Here's how the company shares, monetizes, and exploits it », 19 mars 2020. Ces entreprises vendent les espaces publicitaires en « real-time bidding ». Cette technique consiste à vendre, en temps réel et au plus offrant, une impression publicitaire donnée.

432. Les contrats de cession de données personnelles. En 2013, la chambre commerciale de la Cour de cassation avait affirmé, dans une décision remarquée, que « tout fichier informatisé contenant des données à caractère personnel doit faire l'objet d'une déclaration auprès de la CNIL et que la vente par la société Bout-Chard d'un tel fichier qui, n'ayant pas été déclaré, n'était pas dans le commerce, avait un objet illicite »[1619]. En annulant le contrat de cession de clientèle pour manquement aux obligations déclaratives, cette décision laissait penser que le droit des données personnelles était érigé comme une nouvelle source du droit des contrats[1620]. Toutefois, et comme l'ont remarqué plusieurs auteurs, l'approche formelle retenue par la Cour de cassation est une occasion manquée pour le juge judiciaire de s'investir pleinement dans la mise en œuvre du droit Informatique et libertés[1621].

En s'attachant au seul contrôle des obligations déclaratives[1622], cette décision a rapidement montré ses limites[1623]. D'une part, déjà à l'époque de la décision, la garantie constituée par le respect des formalités déclaratives était légère, surtout en matière de fichiers clients[1624]. En effet, ces traitements devaient seulement faire l'objet d'une déclaration simplifiée auprès de la CNIL. Une fois la déclaration effectuée, l'institution délivrait sans délai un récépissé sans exercer un contrôle de fond sur la licéité du traitement[1625]. C'est ce qui explique que la concordance entre la formalité déclarative et le respect des règles de fond était loin d'être évidente pour ces traitements. D'autre part, la disparition des formalités déclaratives, actée par l'entrée en application du règlement européen[1626], témoigne du champ limité de la solution de 2013 et de son obsolescence. En effet, une lecture littérale de l'arrêt de 2013 empêche d'étendre la qualification de chose hors-commerce aux traitements ne respectant pas les règles de

---

[1619] Cass. com., 25 juin 2013, nº 12-17.037, *Bull.* 2013, IV, nº 108. Pour des analyses de cet arrêt v. not. S. Gaudemet, « Nullité du contrat pour objet illicite. Un nouveau venu parmi les choses hors du commerce : le fichier non déclaré à la CNIL », *Revue juridique de l'économie publique* 2014, nº 717, comm. 12 ; A. Debet, « Un fichier non déclaré à la CNIL est une chose hors du commerce », *JCP G* 2013, nº 37, p. 930 ; J. Rochfeld, « Une nouvelle source en droit des contrats : la loi Informatique et libertés », *RDC* 2014, nº 1, p. 119.

[1620] J. Rochfeld, « Une nouvelle source en droit des contrats : la loi Informatique et libertés », *RDC* 2014, nº 1, p. 119.

[1621] A. Debet, « Un fichier non déclaré à la CNIL est une chose hors du commerce », *JCP G* 2013, nº 37, p. 930 et C. Alleaume, « Les données à caractère personnel comme objet de contrats », *AJ Contrat* 2019, p. 373.

[1622] La Cour de cassation caractérise l'illicéité de l'objet par le manquement aux règles déclaratives.

[1623] Pour une analyse sur les conséquences de cette décision dans le domaine du droit des affaires, v. J.-B. Seube, « La vente d'un fichier informatisé de clients non déclaré à la CNIL est annulée pour illicéité de son objet », *JCP E* juill. 2013, nº 29, p. 1422.

[1624] Ces traitements entraient dans le champ d'une norme simplifiée liée à la gestion de clients et de prospects. Les obligations déclaratives étaient donc allégées, v. CNIL, délibération nº 2016-264 du 21 juillet 2016 portant modification d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects.

[1625] A. Debet, « Un fichier non déclaré à la CNIL est une chose hors du commerce », *JCP G* sept. 2013, nº 37, p. 930.

[1626] V. *supra*, nºs 312 s.

fond de cette matière[1627]. Ainsi, cette solution n'apporte pas les garanties juridiques nécessaires à la protection effective des personnes concernées par ces transmissions de données. Il apparaît que les risques liés à ces transmissions n'ont pas été suffisamment encadrés par le règlement européen.

433. L'imprécision des règles entourant la cession de fichiers clients. Les règles actuelles ne sont pas toujours claires sur les conditions entourant la cession de fichiers de données à caractère personnel. Pourtant, la cession de fichiers client, autrement dit les informations recueillies sur la clientèle d'un marché particulier ou général, est une opération courante[1628].

Longtemps, la doctrine a considéré les obligations déclaratives comme étant la principale limite à ces cessions[1629]. L'abandon de ces obligations, acté par l'entrée en application des nouvelles normes, interroge donc sur les limites actuelles applicables à ces cessions de fichiers. Dans sa norme simplifiée de 2016 sur cette question, la CNIL ne prévoyait pas de règle particulière quant à un éventuel recueil du consentement en cas de cession de données[1630]. Les avocats sont divisés sur cette question. Certains d'entre eux considèrent que le cédant doit réitérer le consentement du client à l'occasion de la cession, sauf si, lors de la collecte initiale, il avait anticipé une telle cession[1631]. Qu'en est-il si le traitement initial n'était pas fondé sur le consentement de la personne concernée mais plutôt sur l'intérêt légitime ou sur le contrat ? Ainsi, d'autres avocats considèrent que c'est plutôt au cessionnaire que revient l'obligation d'informer les personnes concernées de son identité et de la cession de leurs données. Le cessionnaire devrait également obtenir le consentement à la cession des données, « à moins qu'un intérêt légitime puisse se justifier, auquel cas les personnes concernées disposent toujours de la faculté de s'opposer à la transmission de leurs données »[1632]. Dans tous les cas, il y a fort à parier que si les personnes concernées doivent, par un acte exprès, formuler un consentement à la cession, le fichier de clients risque d'être

---

[1627] C. Alleaume, « Les données à caractère personnel comme objet de contrats », *AJ Contrat* 2019, p. 373. Comp. V. Bonnard, « Licence et cession de bases de données personnelles sont-elles compatibles avec le RGPD ? », *DPO consulting* oct. 2018.
[1628] *Rép. civ.* Dalloz, *V°* « Clientèle. Opérations sur la clientèle », par H. Barbier et J. Heinich, 2016, n° 84.
[1629] *JCl. entreprise individuelle,* fasc. 1932, « Fonds de commerce. Fonds de commerce électronique. Cession », par S. Castagné, 2014 (actu. 2017), n^os^ 33 s. ; *Rép. civ.* Dalloz, *V°* « Clientèle. Opérations sur la clientèle », par H. Barbier et J. Heinich, 2016, n° 85.
[1630] CNIL, délibération n° 2016-264 du 21 juillet 2016 portant modification d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects.
[1631] Gouache, « Fonds de commerce, fichiers-clients et RGPD », nov. 2019.
[1632] A. Bounedjoum et J. Guillé, « Comment transmettre un fichier clients en conformité avec le RGPD dans le cadre d'une cession de fonds de commerce exploité en franchise ? », *La Lettre des Réseaux* 5 nov. 2019.

considérablement réduit et sa valeur sera probablement tout autant diminuée. Ainsi, les obligations entourant ces cessions sont relativement incertaines et les transferts de données risquent donc de se poursuivre.

434. Les risques liés aux acquisitions d'organismes. Aux questions relatives à la communication des données à des tiers s'ajoutent également les enjeux liés aux acquisitions effectuées par des grandes entreprises du numérique, notamment dans le but d'étoffer et diversifier les données collectées sur leurs utilisateurs[1633]. L'acquisition par Facebook de l'entreprise WhatsApp en 2014 est une illustration intéressante de ces enjeux[1634]. Deux ans après cet achat, et pour tenir compte du fait que les données des utilisateurs de l'application WhatsApp étaient transmises à Facebook, l'application WhatsApp avait mis à jour ses conditions d'utilisation ainsi que sa politique de confidentialité afin d'informer les utilisateurs de ce transfert. Dans une mise en demeure du 27 novembre 2017[1635], la CNIL avait qualifié Facebook de « destinataire des données à caractère personnel collectées par la société WhatsApp », et avait affirmé que la transmission de ces données était privée de fondement valable, et donc illicite[1636]. Il semble que les actions coordonnées et la mobilisation sans précédent des autorités nationales de contrôle, notamment italienne, anglaise, française et allemande[1637], ont poussé WhatsApp à suspendre ces transmissions[1638]. La mobilisation citoyenne et les contrôles opérés par les autorités sont donc indispensables pour garantir le respect du droit des données à caractère personnel.

[1633] La diffusion de cette pratique s'explique facilement : les start-up sont souvent financées par des fonds de capital-risque (*venture capital*), ce qui rend leur modèle économique instable et précaire. Lorsque les start-up collectent des données sur les utilisateurs, il est fréquent qu'elles ne réussissent pas à les monétiser seule. C'est pourquoi, quand leurs bases de données sont suffisamment fournies, certaines grandes entreprises peuvent être intéressées et proposer un achat.

[1634] L'achat par Facebook de l'entreprise Instagram en 2012 amenait à se poser des questions similaires. D'ailleurs, la FTC avait enquêté sur cette acquisition, FTC, « FTC closes its investigation into Facebook's proposed acquisition of Instagram photo sharing program », 22 août 2012.

[1635] CNIL, décision n° 2017-075 du 27 novembre 2017, mettant en demeure la société WhatsApp.

[1636] Comme le remarque Madame Anne Debet, « la CNIL semble considérer la transmission des données à Facebook comme un traitement à part entière et non comme une finalité du traitement mis en œuvre par WhatsApp (…). Dans différents documents, cependant, le G29 semblait plutôt envisager la transmission comme une finalité », v. A. Debet, « Dans la famille Facebook, la CNIL s'intéresse désormais à WhatsApp », *CCE* 2018, n° 5, comm. 38, citant G29, WP 187, Avis 15/2011 relatif à la définition du consentement, 13 juill. 2011, p. 2.

[1637] En Angleterre, l'autorité de protection des données personnelles (Information Commissioner's Office) avait enquêté sur les implications de cette acquisition. En Allemagne, l'autorité de protection des données personnelles de Hambourg, confirmée par la cour administrative, avait enjoint à Facebook d'arrêter l'importation de données et de supprimer les informations déjà collectées. En Italie, WhatsApp avait été condamné à une amende de 3 millions d'euros par l'autorité de la concurrence pour ce défaut d'information. Pour un panorama de ces décisions, v. J. Lausson, « Facebook n'entend pas renoncer aux données personnelles de WhatsApp malgré le RGPD », *Numerama* 15 mars 2018.

[1638] WhatsApp, « Undertaking », 12 mars 2018.

Plus largement, ces acquisitions posent des questions quant à la centralisation au sein d'un même groupe, sur le long terme, de données à caractère personnel[1639]. Certaines des règles du droit de la concurrence peuvent être utilement mobilisées[1640]. Par exemple, les règles liées à la concentration, c'est-à-dire l'opération par laquelle un changement durable du contrôle d'une entreprise est réalisé[1641], pourraient éviter des entraves significatives à la concurrence et, par ricochet, une centralisation des données personnelles[1642]. À ce propos, il est intéressant de remarquer qu'une décision allemande s'est fondée sur le droit de la concurrence pour affirmer que Facebook avait abusé de sa position dominante sur le marché des réseaux sociaux afin de collecter des données personnelles[1643]. Ces questions amènent à s'interroger sur les véritables garanties dont les personnes peuvent bénéficier lorsque leurs données font l'objet de transmissions.

435. L'insuffisance des règles entourant les communications de données personnelles aux « destinataires ». Les règles actuelles entourant la communication de données personnelles à des destinataires sont relativement permissives. Les obligations les plus contraignantes pour ces traitements sont principalement de deux ordres. D'une part, la question du fondement de licéité du nouveau traitement se pose pour le destinataire. Les incertitudes liées à cette recherche de fondement risquent d'encourager des manquements au droit des données personnelles. En effet, il est fréquent de constater que les tiers auxquels les données ont été transmises ne respectent pas leurs obligations[1644]. Ces manquements sont difficiles à déceler du fait de l'absence de traçabilité technique des données. D'autre part, la mise en œuvre de l'obligation d'information de la personne concernée lors de la transmission de ses données

---

[1639] V. sur cette question, B. Thompson, « Data Factories », *Stratechery* 2 oct. 2018.
[1640] G. Colangelo et M. Maggiolino, « Data accumulation and the privacy – antitrust interface : insights from the Facebook case », *International Data Privacy Law* 2018, vol. 8, p. 224 s. Le Congrès américain a publié un rapport très complet suite à son enquête dédiée aux questions de libre concurrence dans les marchés numériques, J. Nadler *et al.*, « Investigation of competition in digital markets. Majority staff report and recommandations », House of Representatives, 2020.
[1641] Ce changement peut résulter, soit d'une fusion de deux ou de plusieurs entreprises (ou de parties d'entre elles), soit de l'acquisition, par une ou plusieurs personnes du contrôle, direct ou indirect, d'une ou de plusieurs entreprises, v. art. 3 du règlement CE nº 139/2004 du 20 janv. 2004 relatif au contrôle des concentrations entre entreprises, *JOUE* 29 janv. 2004, L-24/1, p. 1 s.
[1642] N. Laneret, R. Knittel et A. Baudequin, « Protection des données personnelles : quand le droit de la concurrence s'en mêle », *Dalloz IP/IT* 2017, p. 619.
[1643] A. Satariano, « Facebook loses antitrust decision in Germany over data collection », *The New York Times* 23 juin 2020. Pour une étude analysant les effets du droit des données personnelles sur la concentration, v. G. Johnson, S. Shriver et S. Golberg, « Privacy & market concentration : intended & unintended consequences of the GDPR », juill. 2020. L'autorité de la concurrence française vient d'ailleurs de créer un service dédié au numérique, Autorité de la concurrence, « L'autorité crée un service de l'économique numérique », 9 janv. 2020.
[1644] Sur les manquements aux obligations d'information, v. Conseil d'État, « Le numérique et les droits fondamentaux », *Rapport Public 2014*, La Documentation française, 2014, p. 183.

personnelles à des destinataires ou à des catégories de destinataires engendre également des difficultés[1645]. Parce que le législateur fait référence aux « catégories » de destinataires, les responsables du traitement peuvent fournir aux personnes concernées une information nébuleuse et lapidaire, les empêchant en réalité d'avoir une vision nette des organismes ayant eu accès à leurs données personnelles.

Souvent, cette information est consignée dans de longues et complexes politiques de confidentialité empêchant la personne concernée d'identifier simplement avec quels destinataires le responsable du traitement a partagé ses informations. Par exemple, dans sa politique de confidentialité, l'entreprise Facebook annonce de manière évasive qu'elle collabore « avec des partenaires tiers qui nous aident à fournir et à améliorer nos produits ou qui utilisent les outils professionnels Facebook pour développer leur activité, ce qui nous permet d'exploiter nos sociétés et de proposer des services gratuits dans le monde entier »[1646]. En aucun cas ce type de phrases, présentes dans la plupart des politiques de confidentialité, ne permet à la personne concernée de savoir à quelles entreprises ses données sont communiquées[1647]. Une telle approche empêche les personnes d'avoir, à l'égard de leurs données, un quelconque pouvoir. Conformément aux études ayant démontré que les politiques de confidentialité ne permettent pas d'informer concrètement les consommateurs des utilisations de leurs données[1648], le règlement européen a prévu que les informations relatives au traitement des données doivent être « aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples »[1649]. En dépit de l'entrée en application de ce texte depuis

---

[1645] Art. 13 du règlement UE nº 2016/679. Depuis juillet 2019, conformément à l'article 14 du règlement UE nº 2016/679, Facebook propose à ses utilisateurs de connaître les entreprises ayant vendu l'accès aux données personnelles à un annonceur, v. L. Ronfaut, « Sur Facebook, on peut savoir quelles entreprises ont revendu nos données à des annonceurs », *Le Figaro* 11 juillet 2019.

[1646] La politique de confidentialité de Facebook énumère sept catégories de « partenaires tiers » parmi lesquels sont mélangés les destinataires de données (au sein desquels figurent de manière indifférenciée les fournisseurs et prestataires de services ou les annonceurs et les chercheurs et universitaires) et les tiers autorisés (tels que les forces de l'ordre ou les cas de demandes légales), v. Facebook, « Politique d'utilisation des données. Comment ces informations sont-elles partagées ? », consultée le 29 oct. 2020. En avril 2019, Facebook a proposé une nouvelle fonctionnalité permettant aux utilisateurs de comprendre pourquoi les publications apparaissent dans leur fil d'actualité, v. Facebook, « Facebook lance la fonctionnalité "Pourquoi est-ce que je vois ça ?" dans le fil d'actualité », avr. 2019.

[1647] La partie dédiée à cette question de la politique de confidentialité de l'entreprise TikTok particulièrement populaire est tout aussi nébuleuse, v. TikTok, « How we share your personal data », in *Privacy policy*, juin 2020.

[1648] Selon une étude de 2008, il faudrait 244 heures par an pour lire les politiques de confidentialité des sites visités, v. A. McDonald et L. Faith Cranor, « The cost of reading privacy policies », *I/S: a journal of law and policy* 2008, vol. 4 : 3, p. 544, spéc. p. 563. Sur l'ineffectivité des politiques de confidentialité pour la protection des personnes, v. F. Schaub, R. Baleko et L. Faith Cranor, « Designing effective privacy notices and controls », *IEEE Internet Computing* 2017 ; F. Schaub, « Nobody reads privacy policies. Here's how to fix that », *The Conversation* 10 oct. 2017. Sur les difficultés de compréhension des politiques de confidentialité, v. K. Litman-Navarro, « We read 150 privacy policies. They were an incomprehensible disaster », *The New York Times* 12 juin 2019.

[1649] Cons. 39 du règlement UE nº 2016/679. Sur l'interprétation retenue par le G29 du principe de transparence, v. G29, WP 260 rév. 01, Lignes directrices sur la transparence au sens du règlement 2016/679, 11 avr. 2018, p. 15.

plusieurs années, l'information fournie aux personnes concernées reste toujours très obscure[1650]. La complexité de l'information communiquée aux personnes concernées, cumulée aux pratiques d'un grand nombre de ces destinataires, génère des risques importants pour les personnes.

436. Les atteintes à la protection des personnes. La communication de données personnelles à des destinataires porte atteinte à la protection des personnes garantie par le droit des données personnelles. En effet, l'information générale communiquée aux personnes concernées les empêche de connaître la liste exhaustive des tiers ayant reçu communication de leurs données. La plupart du temps, les personnes concernées n'ont même pas conscience que leurs données sont transmises à des tiers[1651]. Cette obscurité porte atteinte à la capacité des personnes d'exercer un véritable *contrôle* à l'égard de leurs données. En effet, l'ignorance dans laquelle elles sont placées porte atteinte à leur pouvoir de contrôle sur les modalités de divulgation de leurs données. Par ailleurs, cette ignorance les empêche de s'assurer que les destinataires respectent effectivement le droit des données personnelles, notamment leur obligation d'information prévue par l'article 14 du règlement européen[1652]. En effet, il leur est impossible de s'assurer du respect de leurs droits si elles ne savent pas que leurs données font l'objet de traitement. En plus de porter atteinte au pouvoir de contrôle, ces communications renforcent le sentiment d'impuissance des personnes à l'égard de leurs données. Ces transmissions doivent donc être mieux encadrés.

B. De lege ferenda : un encadrement strict

437. Renforcer l'obligation de transparence. Pour que la personne puisse exercer un véritable contrôle sur ses données, il est indispensable qu'elle ait connaissance des entités qui les traitent. Actuellement, l'information transmise est insuffisante pour garantir un tel contrôle. Il faut donc affiner les obligations de transparence en obligeant les responsables du traitement à fournir une *liste exhaustive* des destinataires ayant reçu

[1650] En 2019, la CNIL a sanctionné l'entreprise Google à hauteur de 50 millions d'euros notamment pour des manquements de ce type, v. CNIL, délibération n° 2019-001 du 21 janvier 2019 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google LLC, § 189.
[1651] Sur l'absence de conscience de l'individu du traitement de ses données, v. not. J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 148 s.
[1652] L'article 14 du règlement UE n° 679/2016 est relatif aux informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée.

communication de données personnelles[1653]. Le responsable du traitement devrait ainsi être tenu d'identifier chaque destinataire de manière distincte pour permettre à la personne concernée de suivre ses données et de vérifier le respect par ces destinataires de leurs obligations. Ainsi, la référence aux catégories de destinataires, dans les articles 13, 14, 15 et 30 du règlement européen, devrait être supprimée.

438. Une transmission aux destinataires soumise au consentement de la personne concernée. En plus du renforcement du principe de transparence, le principe de *privacy by default* devrait également être mieux garanti dans le cadre des communications de données[1654]. Ce principe, prévu par le deuxième paragraphe de l'article 25 du règlement européen, implique de définir le niveau de protection maximale et de s'assurer que la solution technique garantit cette protection sans qu'un réglage par l'utilisateur ne soit nécessaire[1655]. Une interprétation stricte de ce principe implique donc que, par défaut, le responsable du traitement limite scrupuleusement les effets intrusifs ou portant atteinte aux libertés de la personne de ses traitements[1656]. Transposé aux communications de données, ce principe pourrait être interprété de telle façon que, par principe, les transferts de données vers des destinataires ne sont pas permis. D'ailleurs, la référence dans l'article 25 du règlement européen à l'interdiction de diffusion de données personnelles en l'absence d'intervention de la personne concernée, est le signe des liens qu'entretiennent la *privacy by default* et la communication de données à caractère personnel[1657]. Une interprétation large de cette disposition permet donc de considérer que les communications aux destinataires ne peuvent se faire qu'après une intervention de la personne concernée. En d'autres termes, pour la plupart des transmissions, seul un consentement libre, éclairé, explicite et spécifique devrait permettre la communication de données à des destinataires[1658]. Ce consentement

[1653] Une telle liste pourrait également servir dans d'autres domaines, notamment en droit de la concurrence afin de voir les coopérations entre les organismes et éventuellement déceler des manquements à ce droit.
[1654] Art. 25 du règlement UE nº 679/2016. V. déjà sur ce principe, A. Cavoukian, « Privacy by design in law, policy and practice. A white paper for regulators, decision-makers and policy-makers », 2011.
[1655] L. Godefroy, « Le code algorithmique au service du droit », *D.* 2018, p. 734.
[1656] M. Griguer et J. Schwartz, « Privacy by design / Privacy by default. Une obligation de conformité et un avantage concurrentiel », *Cahiers de droit de l'entreprise* 2017, nº 3, p. 74.
[1657] L'article 25 § 2 du règlement UE nº 2016/679 affirme que « ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée ».
[1658] Dans son analyse sur l'achat de WhatsApp par Facebook, la CNIL avait envisagé deux fondements pour justifier la transmission des données entre les entreprises. D'une part, elle avait examiné le consentement pour ensuite considérer que celui-ci ne présentait pas les qualités requises. D'autre part, elle avait envisagé l'intérêt légitime, qu'elle n'avait pas considéré comme suffisant pour justifier les atteintes aux personnes engendrées par cette transmission, v. CNIL, décision nº 2017-075 du 27 nov. 2017 mettant en demeure la société WhatsApp. Pour

pourrait être recueilli par l'intermédiaire d'une case à cocher (non pré-cochée par défaut), et ne devrait pas résulter de l'acceptation de conditions générales[1659]. Il est fort probable d'anticiper une baisse importante du nombre de données transférées. En effet, il est possible de prédire que si la personne a bien compris la question, elle refusera probablement le transfert[1660].

439. Les mesures techniques. De manière provocante, Messieurs Alain Rallet et Fabrice Rochelandet affirmaient que la régulation est relativement impuissante face à la circulation généralisée des données[1661]. Dans une certaine mesure, cette affirmation se vérifie toujours puisque la régulation n'a pas empêché les courtiers de données de prospérer en Europe[1662], et que les transferts de données personnelles entre organismes sont courants. Bien sûr, il convient de distinguer les situations qui génèrent une insécurité juridique telle que les organismes appliquent à leur avantage certaines règles, et les cas dans lesquels les organismes agissent purement et simplement dans l'illégalité assumée. En tout état de cause, pour pallier ces problèmes de suivi et d'accès aux données évoqués, des propositions techniques peuvent être brièvement exposées.

440. La coloration des données. La première mesure technique est celle d'une coloration des données[1663] permettant de suivre leur circulation et d'établir leur provenance[1664]. Un tel système technique colorerait la donnée afin de suivre les traces qu'elle laisse lorsqu'elle est dupliquée, modifiée ou transférée, permettant ainsi à

---

une analyse de cette décision : v. not. A. Debet, « Dans la famille Facebook, la CNIL s'intéresse désormais à WhatsApp », *CCE* 2018, nº 5, comm. 38.

[1659] A. Debet, « Les nouveaux instruments de conformité », *Dalloz IP/IT* 2016, p. 592. Sur l'importance du principe d'opt-in pour la protection des personnes, v. *supra*, nº 376.

[1660] Cette intuition se confirme puisque, depuis les mises à jour du logiciel iOS permettant aux détenteurs d'iPhone de désactiver le suivi de localisation ou de rendre le traçage plus visible, la collecte de ces données a été drastiquement réduite, v. *supra*, nº 376.

[1661] A. Rallet et F. Rochelandet, « La régulation des données personnelles face au web relationnel : une voie sans issue ? », *Réseaux* 2011, nº 167, p. 40.

[1662] V. *supra*, nº 431.

[1663] Cette expression renvoie au processus plus large de *data lineage* qui permet de décrire le détail des règles de transformation de la donnée de la source jusqu'à la restitution, G. Abisror, « Le data lineage, un levier important d'efficacité opérationnelle et de réduction des risques », *Deloitte*. Ce traçage permet une visualisation du cycle de vie de la donnée pour savoir de quelle source provient une donnée et quelles transformations elle a subies.

[1664] Les sénateurs Gaëtan Gorce et François Pillet avait retenu une expression similaire (le marquage de données) pour répondre au risque de propagation d'erreur dans des bases de données ouvertes. Pour autant, les sénateurs évoquent ensuite des exemples d'enregistrement des personnes ayant eu accès aux données (et non pas le marquage de la donnée en tant que telle), puisqu'ils envisagent « l'archivage, par l'administration, des coordonnées des réutilisateurs », v. G. Gorce et F. Pillet, « Rapport d'information sur l'open data et la protection de la vie privée », Sénat, nº 469, 16 avr. 2014, p. 65.

l'utilisateur de suivre « à la trace » ses données[1665]. Tel le Petit Poucet laissant sur son passage les petits cailloux blancs pour retrouver son chemin, la donnée laisserait sur son passage une couleur permettant de la suivre et de retrouver les endroits par lesquels elle est passée.

441. Une meilleure étanchéité des données. En plus de ce système de traçage, des protocoles garantissant une plus grande étanchéité des données pourraient également être mis en place[1666]. Par exemple, les données pourraient être chiffrées de telle façon que la personne concernée soit la seule à pouvoir attribuer les clés de déchiffrement aux destinataires auxquels elle souhaite permettre l'accès[1667]. Ces mécanismes de chiffrement des données offriraient aux personnes un meilleur contrôle de leurs données.

À ces mécanismes de chiffrement des données pourrait s'ajouter un système de « tableau de bord de la vie privée », permettant à l'utilisateur de voir quelles ont été les données qui ont été collectées, qui y a eu accès et, le cas échéant, de révoquer ces accès[1668]. Ces tableaux de bord, déjà mis en œuvre par certaines entreprises, permettent aux utilisateurs d'avoir une vision plus fine des accès à leurs données et un meilleur contrôle sur celles-ci[1669]. Leur utilité doit toutefois être relativisée pour au moins deux raisons. D'une part, ces tableaux n'offrent qu'un contrôle limité à l'utilisateur puisque les paramètres de « contrôle » sont définis de manière unilatérale par les organismes[1670]. D'autre part, pour garantir l'effectivité de la protection des personnes, c'est surtout les paramètres par défaut qui sont importants puisque la plupart des personnes ne les modifient pas[1671].

[1665] Des chercheurs ont eu recours à cette méthode pour montrer les failles de données personnelles, L. Li, A. Bartel, J. Klein, Y. Le Traon, S. Arzt, S. Rasthofer, E. Bodden, D. Octeau et P. Mcdaniel, « I know what leaked in your pocket : uncovering privacy leaks on Android Apps with Static Taint Analysis », 2014.
[1666] V. not. L. Merzeau, « De la surveillance à la veille », in dossier « Internet et la société de contrôle : le piège ? », dir. R. Damien et P. Mathias, *Cités* 2009, nº 39, p. 67, spéc. p. 79.
[1667] Pour un exemple de technologie permettant ce type de chiffrement de bout en bout, v. Tresorit, « Security Whitepaper », 2013.
[1668] J. Rochfeld, « La vie tracée ou le code civil doit-il protéger la présence numérique des personnes », in *Mélanges J. Hauser*, Dalloz, 2012, p. 619 s., nº 17, spéc. p. 637.
[1669] Par exemple, Google a lancé le tableau de bord de la vie privée en novembre 2009, Google, « Transparency, choice and control – now complete with a Dashboard ! », *Google official blog* 5 nov. 2009 ; Microsoft a également offert cette possibilité en 2017 avec le lancement de Windows 10, T. Myerson, « Our continuing commitment to your privacy with Windows 10 », *Windows Blogs* 10 janv. 2017.
[1670] W. Hartzog, « Control is not the privacy solution it's made out to be », 18 janv. 2019.
[1671] A. Casilli, « Contre l'hypothèse de la "fin de la vie privée". La négociation de la *privacy* dans les médias sociaux », *Revue française des sciences de l'information et de la communication* 2013, nº 3.

À ces propositions techniques et juridiques doivent impérativement s'ajouter un renforcement des contrôles et des mesures réparatrices[1672]. En effet, seule une vigilance des autorités de contrôle et des juges garantissent le respect effectif des principes de protection des personnes prévus par le droit des données personnelles.

Pour rendre réel le pouvoir de contrôle des personnes à l'égard de leurs données, il convient donc d'encadrer les accès aux données par les destinataires. L'encadrement du droit à l'oubli et de l'accès aux données par les tiers est nécessaire pour garantir un équilibre entre les intérêts au cœur du droit des données. À cet encadrement doit également s'ajouter un raffermissement de certains principes de cette matière.

SECTION II – RAFFERMIR DES PRINCIPES

442. Des principes insuffisants. La meilleure façon de protéger les données, c'est de ne pas les collecter. La proposition paraît simplificatrice, pourtant, elle énonce une opinion fréquemment occultée par les promesses du *big data*[1673]. Une meilleure protection des personnes passe donc par une collecte restreinte de leurs données. Le droit des données à caractère personnel reconnaît d'ores et déjà un tel principe, bien que sa mise en œuvre soit souvent mise à mal par les technologies « datavores » et les promesses qu'elles emportent avec elles. Par ailleurs, le plus souvent, cette collecte de données n'est que la première étape d'un processus plus étendu ayant pour objectif une personnalisation des services[1674]. Insidieusement, les décisions fondées sur des traitements automatisés se diffusent. À nouveau, le droit positif prévoit un encadrement de ces traitements. Toutefois, la pratique montre les limites de ces règles et met en exergue leurs lacunes.

443. Plan. Les principes de minimisation et ceux liés aux décisions fondées sur des algorithmes sont ébranlés par les pratiques numériques. Ils sont pourtant essentiels dans la protection des personnes à l'ère des traitements massifs de données. L'étude du principe de minimisation (§ I) précèdera celle des règles encadrant les prises de décision fondées sur des traitements automatisés (§ II).

[1672] Sur l'importance des contrôles et de mise en œuvre de la responsabilité, v. *infra*, n^os^ 463 s.
[1673] Cette expression évoque « la constitution et l'exploitation de grandes masses de données dans le but de les transformer en information », A. Bensamoun et C. Zolynski, « *Big data* et *privacy* : comment concilier nouveaux modèles d'affaires et droits des utilisateurs ? », colloque *Transformations sociales et ère numérique* du Forum mondial des sciences sociales, Montréal, 15 oct. 2013, *LPA* 18 août 2014, n^o^ 164, p. 8, § 1.
[1674] V. *supra*, n^o^ 389

§ I. Le principe de minimisation

444. Origines du principe de minimisation. Le principe de finalité et son corollaire, celui de proportionnalité, sont apparus avec la Convention 108[1675] et ont été repris par la directive 95/46[1676]. Ils n'étaient pas explicitement formulés dans la loi du 6 janvier 1978, mais se retrouvaient, de manière implicite, dans les règles relatives aux formalités[1677]. En effet, les responsables du traitement devaient déclarer la finalité du traitement, et tout détournement pouvait faire l'objet d'une sanction pénale[1678].

Le principe de finalité, repris par le règlement européen, impose au responsable du traitement de déterminer, avant tout traitement de données, la raison pour laquelle il souhaite le mettre en œuvre[1679]. Le pendant de ce principe est le « test de proportionnalité » que le responsable du traitement doit effectuer afin de vérifier qu'il ne traite que les données « pertinentes, adéquates et non excessives »[1680].

Une opinion doctrinale a considéré que le test de proportionnalité prévu par la directive 95/46 devait être interprété comme un principe de minimisation des données, c'est-à-dire comme restreignant la collecte au *minimum nécessaire*[1681]. À l'inverse, d'autres auteurs ont considéré qu'une telle interprétation restrictive ne découlait pas de la lettre de la directive puisque l'exigence selon laquelle les données ne doivent pas être excessives n'interdit pas la collecte de données utiles mais non strictement nécessaires, comme par exemple la collecte d'informations destinées à effectuer de la prospection commerciale[1682]. Le législateur européen a tranché ce débat en retenant l'interprétation la plus restrictive du principe de proportionnalité. En effet, l'article 5

[1675] Art. 5 b) et c) de la Convention 108.
[1676] Art. 6 b) et c) de la directive CE nº 95/46.
[1677] D'ailleurs, selon Monsieur Jean Frayssinet, le principe de finalité ne serait rien de moins que la « colonne vertébrale de la loi Informatique et libertés », v. J. Frayssinet, *Informatique, fichiers et libertés*, Litec, 1992, nº 172, p. 73. Le principe de proportionnalité était également présent dans la loi Informatique et libertés puisque le rapport Tricot énonçait que « l'adéquation des données à la finalité doit être une idée directrice, plus féconde, croyons-nous, que les interdictions *a priori* », B. Tricot, « Rapport de la commission Informatique et libertés », La Documentation française, 1975, p. 46.
[1678] Art. 44 de la loi nº 78-17 du 6 janv. 1978.
[1679] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nºs 693 s., p. 287 s. Sur les apports limités du règlement européen, F. Gaullier, « Le principe de finalité dans le RGPD : beaucoup d'ancien et un peu de nouveau », *CCE* 2018, nº 4, dossier 10.
[1680] Art. 5 c) de la Convention 108, art. 5 c) de la directive CE nº 95/46 et art. 5 § 1 c) du règlement UE nº 2016/679. Cela renvoie d'ailleurs au principe de pertinence, c'est-à-dire l'exigence que « l'étendue de la connaissance accessible à autrui soit strictement proportionnée à une finalité légitime définie prioritairement par référence à la nature de la relation en cause », D. Gutmann, *Le sentiment d'identité. Étude de droit des personnes et de la famille*, th. Paris II, 2000, LGDJ, nº 287, p. 249.
[1681] C. Kuner, *European Data Protection Law : Corporate Compliance and Regulation*, 2e éd., OUP Oxford, 2007, nº 2.30, p. 73 s.
[1682] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 748, p. 305.

du règlement européen fait désormais explicitement référence au principe de minimisation, et l'article 25 de ce texte le reprend comme élément essentiel de la *privacy by design*[1683]. Il est donc établi que le test de proportionnalité exige que seules les données strictement nécessaires aux finalités préalablement déterminées puissent être collectées.

Un tel principe contribue à l'établissement d'un rapport de confiance entre le responsable du traitement et la personne concernée, qui devrait être invitée à fournir uniquement les données nécessaires au service. Par exemple, la personne concernée comprend qu'à l'occasion d'un envoi de colis, les services postaux lui demandent les adresses postales de l'expéditeur et du destinataire. En revanche, cette confiance pourrait s'éroder si l'expéditeur était sommé de fournir d'autres informations sans lien avec le service, telles qu'une date de naissance ou un document d'identité[1684]. Cette collecte non nécessaire pourrait entamer sa confiance à l'égard du responsable du traitement et porter atteinte à d'autres principes du droit des données personnelles[1685].

445. Le principe de minimisation, ébranlé par les pratiques numériques. Le principe de minimisation s'oppose frontalement à la tendance actuelle des responsables du traitement voyant, dans la collecte massive et généralisée de données, une potentielle « mine d'or future »[1686] qu'ils pourraient exploiter grâce aux technologies liées au *big data*[1687]. Le présupposé sur lequel repose ces technologies s'appuie sur l'idée que l'utilité des données se manifeste en cours de traitement et que toute donnée, même triviale, participe à la création et à l'amélioration des profils[1688]. À la différence des traitements statistiques classiques, dans lesquelles les hypothèses précèdent et

---

[1683] Art. 25 du règlement UE nº 2016/679.
[1684] Cela rejoint d'ailleurs l'interprétation de la condition de licéité du contrat qui permet de collecter seulement les données strictement nécessaires à l'exécution du contrat, CEPD, Lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées, 8 oct. 2019, § 23 s., p. 9 s. Sur ce point, v. *supra*, nº 365.
[1685] C'est notamment ce que Madame Helen Nissenbaum qualifie comme la *contextual privacy*, H. Nissenbaum, *Privacy rights in context. Technology, policy, and the integrity of social life,* Stanford University Press, 2010, p. 37. Pour un exposé de cette théorie, v. *supra*, nºs 253 s.
[1686] Les données sont souvent présentées comme l'or ou le pétrole du XXIe siècle, v. récemment, M. Clément-Fontaine, « La convergence du droit de la propriété littéraire et artistique et du droit "droit des données" : une fatalité ? », in *Mélanges M. Vivant*, 2020, Dalloz, p. 97 s., spéc. p. 97. La CNIL s'est appropriée cette expression dans deux de ses rapports, CNIL, *Rapport d'activité 2014,* La Documentation française, 2015, p. 72 ; CNIL, *Rapport d'activité 2015,* La Documentation française, 2016, p. 82. Pourtant cette expression fait l'objet de pertinentes critiques, v. not. H. Verdier, « Non, les données ne sont pas du pétrole… », *Henri Verdier Blog*, 19 mars 2013.
[1687] F. Gaullier, « Le principe de finalité dans le RGPD : beaucoup d'ancien et un peu de nouveau », *CCE* 2018, nº 4, dossier 10, § 15.
[1688] A. Rouvroy, « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data », in Conseil d'État, « Le numérique et les droits fondamentaux », *Rapport Public 2014*, La Documentation française, 2014, p. 407.

commandent la collecte de données, les techniques de *big data* visent à faire surgir, grâce aux traitements de grandes quantités de données, des catégories, des modèles prédictifs ou des profils[1689]. Avec ces techniques de traitement de l'information, ce sont les données qui déterminent elles-mêmes les hypothèses et les résultats. C'est pourquoi elles reposent sur une collecte massive, automatique, par défaut, et sur une conservation illimitée de tout ce qui est quantifiable numériquement. Cette collecte est souvent justifiée par le fait que le *big data* améliorerait l'expérience de l'utilisateur et permettrait d'offrir un service adapté et personnalisé[1690]. Face à cet impératif de collecte généralisée, érigé au rang de logique absolue, le principe de minimisation est mis à mal[1691].

446. L'importance du principe de minimisation. Si les pratiques intrusives d'analyse de données sont entrées dans nos vies, cela ne les rend pas pour autant respectueuses des personnes. Au contraire, elles créent de nouveaux dangers pour les libertés individuelles[1692]. En traquant chaque signal, ces traitements font entrer les personnes dans des catégories, et ainsi les enferment dans des modèles décisionnels. Une représentation schématique de ces modèles leur assignerait l'objectif de priver les personnes de leur capacité de choisir : la machine et l'environnement s'adapteraient automatiquement au profil de l'utilisateur, avant même qu'il n'ait à formuler préférence ou intention[1693]. Ces pratiques s'opposent donc à la liberté d'autodétermination dès lors que ces modèles participent à la formation des idées et des sentiments. À l'inverse, le principe de minimisation contribue à préserver cette liberté d'autodétermination et concourt à la mise en œuvre d'autres principes de protection des données.

Tout d'abord, puisque le principe de minimisation diminue les données collectées, les risques de leur centralisation sont plus faibles. Ce principe a donc un impact sur la sécurité des données : puisque celles-ci sont moins nombreuses, les

[1689] A. Rouvroy, « La robotisation de la vie ou la tentation de l'inséparation », in *L'intelligence artificielle et le droit*, dir. H. Jacquemin et A. De Streel, Larcier, 2017, p. 34 s.
[1690] Sur les risques liés à la personnalisation des services, v. *supra*, nº 389.
[1691] Sur les enjeux liés au big data, notamment en lien avec les objets connectés, v. J. Schweiger, « *Smart cities* et nouveaux enjeux de protection des données : comment tirer profit du nouveau règlement européen ? », *Dalloz IP/IT* 2017, p. 624.
[1692] J.-S. Bergé et D. Le Métayer, « Phénomènes de masse et droit des données », *CCE* 2018, nº 12, étude 20, § 4 s. ; L. Marino, « Notre vie privée : des little data aux big data », colloque *Le secret à l'ère de la transparence* organisé par La Semaine Juridique, *JCP G* 2012, supplément au nº 47, p. 14.
[1693] A. Rouvroy, « La robotisation de la vie ou la tentation de l'inséparation », in *L'intelligence artificielle et le droit*, dir. H. Jacquemin et A. De Streel, Larcier, 2017, p. 27.

risques liés à une violation de données sont réduits[1694]. Par ailleurs, les impacts sur la vie privée sont réduits puisque moins de données sont collectées. En diminuant les données collectées, on limite les possibilités de recoupements d'informations, et on évite donc l'identification de personnes par des données très indirectement identifiantes. En ce sens, le principe de minimisation s'inscrit parfaitement dans le prolongement de la nouvelle définition de donnée à caractère personnel[1695]. En effet, dès que le responsable du traitement opère un traitement dont l'objet ou l'effet est de faire un lien avec une personne physique, il est soumis aux principes du droit des données personnelles et donc au principe de minimisation. Il sera donc contraint de trouver une justification pour fonder la collecte de ces informations.

Enfin, le principe de minimisation contribue également à limiter la durée de conservation des données. En effet, en restreignant la collecte aux données strictement nécessaires, on favorise les traitements de données liés à l'exécution de tâches déterminées et on évite donc une conservation longue et généralisée.

Ainsi, le respect du principe de minimisation encadre les modalités de traitements des données personnelles et évite une collecte systématique et potentiellement massive. Il prévient la catégorisation des personnes permettant ensuite d'effectuer des traitements influençant leurs choix. Pour toutes ces raisons, ce principe contribue à une meilleure protection des personnes et doit donc être garanti.

447. Renforcer les contrôles pour favoriser le respect du principe. Actuellement deux dynamiques s'opposent : celle juridique liée au principe de minimisation et celle technologique liée à la volonté d'exhaustivité promue par le *big data*[1696]. Cette dernière dynamique contrevient aux principes du droit et devrait, à ce titre, être mieux encadrée[1697].

L'analyse des mises en demeure et sanctions prononcées par la CNIL depuis 2004 montre que peu d'entre elles visaient effectivement une violation du principe de

[1694] Un attaquant a plutôt intérêt à accéder à une base de données contenant le plus de données possibles. D'ailleurs, le principe de sécurité des données doit être adapté aux risques, dont le degré de probabilité et de gravité varie en fonction des données collectées, v. art. 32 du règlement UE nº 2016/679.
[1695] V. *supra*, nº 273.
[1696] Conseil d'État, « Le numérique et les droits fondamentaux », *Rapport Public 2014*, La Documentation française, 2014, p. 168.
[1697] A. Bensamoun et C. Zolynski, « *Big data* et *privacy* : comment concilier nouveaux modèles d'affaires et droits des utilisateurs ? », colloque *Transformations sociales et ère numérique* du Forum mondial des sciences sociales, Montréal, 15 oct. 2013, *LPA* 18 août 2014, n° 164, p. 8, § 16 s.

finalité[1698]. Pourtant, des contrôles ciblant le respect de ce principe favorisent sa meilleure mise en œuvre. En effet, le sentiment d'impunité des organismes traitant des données les encourage à privilégier la dynamique technologique au détriment de celle juridique. Face à cette tension, des contrôles plus fréquents et plus stricts participent naturellement à une meilleure application des règles. Garantir le respect de ce principe est un impératif, notamment pour prévenir la propagation des décisions fondées sur des traitements automatisés de données.

§ II. Les principes relatifs aux décisions fondées sur des traitements automatisés

448. L'augmentation du nombre de décisions fondées sur des traitements automatisés. En 2017, la mise en demeure de la CNIL sommant le ministère de l'Enseignement supérieur de respecter la loi Informatique et libertés avait fait entrer dans le débat public la question de la prise de décision sur le fondement de traitements de données automatisés[1699]. Le système en cause était celui de la plateforme Admission Post-Bac (APB). Cette plateforme reposait sur un algorithme qui analysait les souhaits d'affectation dans l'enseignement supérieur des élèves de terminale, puis attribuait une place en fonction du domicile, de la situation parentale et de l'ordre de préférence[1700]. La CNIL se saisissait, pour la première fois de manière aussi tranchée, de la question capitale de la prise de décision sur le fondement d'un traitement automatisé[1701]. Pourtant, notre quotidien est envahi d'un nombre toujours croissant de décisions fondées uniquement sur des algorithmes[1702]. Bien sûr, toutes ces décisions n'ont pas les mêmes effets que la décision relative aux études qu'un lycéen a le droit de poursuivre, mais elles peuvent, à force de petits choix, influencer qui nous sommes et surtout qui nous pouvons être. C'est pourquoi la question de l'encadrement de ces décisions est décisive dans l'étude du rôle du droit des données à caractère personnel dans l'effectivité de la protection des personnes.

[1698] La majorité des délibérations de la CNIL qui se référaient aux principes de finalité et de proportionnalité étaient plutôt liées aux obligations d'autorisation préalable, particulièrement celles relatives aux textes réglementaires, v. A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, n^os^ 752 s., p. 307 s. Sur le faible nombre de contrôles effectués par la CNIL, v. *infra*, n° 501.

[1699] CNIL, décision n° 2017-053 du 30 août 2017 mettant en demeure le ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation.

[1700] J. Rochfeld, « L'encadrement des décisions prises par algorithme », *Dalloz IP/IT* 2018, p. 474.

[1701] A. Debet, « APB enfin remis en cause par la CNIL », *CCE* 2017, n° 12, comm. 101.

[1702] Sur l'atteinte à la liberté personnelle par le profilage, v. *supra*, n° 390.

449. Plan. Après avoir étudié l'encadrement actuel des décisions fondées sur des traitements automatisés (A), nous verrons quels sont les risques que l'ensemble des décisions font peser sur les personnes (B) et pourquoi il est impératif de consolider les règles entourant ces décisions (C).

A. L'encadrement des décisions les plus graves

450. Les risques liés aux traitements automatisés, une préoccupation ancienne. Pour éviter que des traitements automatisés de données prennent, de manière autonome, des décisions ayant des répercussions importantes sur les personnes, le législateur avait, dès 1978, adopté des règles pour les encadrer[1703]. Cet encadrement s'est poursuivi puisque l'article 15 de la directive 95/46 reconnaissait à la personne concernée « le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données »[1704]. Cette disposition avait été transposée fidèlement dans l'ancien article 10 de la loi Informatique et libertés[1705].

451. Une mise en œuvre limitée. En dépit du fait que cette disposition était fréquemment invoquée devant la CNIL, l'interdiction était, en pratique, peu respectée[1706]. En effet, l'étude des délibérations de la CNIL montre qu'une faible part d'entre elles se fondaient sur cet article. Ces délibérations retenaient une interprétation relativement indulgente de l'encadrement législatif de ces traitements puisque n'étaient

---

[1703] La place de cette interdiction reflète l'intérêt et la préoccupation du législateur pour cette question. En effet, c'était le deuxième article de la loi Informatique et libertés qui interdisait les décisions de justice, administrative ou privée, impliquant une appréciation sur un comportement humain fondée sur un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé. L'article 3 garantissait, quant à lui, le droit aux personnes de connaître et contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats leur étaient opposés.

[1704] Le second paragraphe de l'article 15 de la directive 95/46 ajoutait deux exceptions : d'une part, si celle-ci était prise dans le cadre de la conclusion ou de l'exécution d'un contrat et lorsque la personne a pu faire valoir son point de vue, et d'autre part, si elle était autorisée par une loi qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée.

[1705] Le législateur français avait repris les principes du texte européen. Toutefois, la loi française avait un champ d'application plus large puisqu'elle faisait référence à « toute décision administrative ou privée » alors que le texte européen ne visait que « une décision produisant des effets juridiques ». Pour encadrer les décisions prises par les établissements de crédit, lesquelles peuvent avoir d'importantes répercussions sur la vie des personnes, la CNIL avait adopté une autorisation unique destinée aux traitements mis en œuvre par ces établissements, délibération n° 2006-019 du 2 février 2006 portant autorisation unique de certains traitements de données à caractère personnel mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit (décision d'autorisation unique n° AU-005) ; et sa modification, v. délibération n° 2008-198 du 9 juillet 2008 modifiant l'autorisation unique n° AU-005 relative à certains traitements de données à caractère personnel mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit.

[1706] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, n^os^ 847 s., p. 338 s.

pas considérées comme des décisions ayant pour seul fondement un traitement de données personnelles celles résultant d'une instruction et prises après que l'intéressé ait pu présenter ses observations[1707], ou encore celles pour lesquelles un humain intervenait, même à un stade très tardif de la prise de décision. En effet, comme le relevait Madame Anne Debet, « la CNIL se contente souvent de la seule existence d'un réexamen humain des refus prononcés sur le fondement d'un traitement en se préoccupant finalement peu des résultats concrets de celui-ci »[1708]. Ainsi, si l'ensemble de la décision était effectué par un algorithme et qu'un humain se contentait de la vérifier, elle n'était pas considérée comme ayant pour seul fondement un traitement de données personnelles. La CNIL s'est montrée accommandante notamment avec les décisions de prêt prises par les établissements bancaires. Il suffisait que le conseiller bancaire vérifie le résultat des taux de prêt décidé par le traitement automatisé et permette à la personne de présenter des observations pour que la décision soit considérée comme licite[1709]. Pourtant, en pratique, ces décisions nient la complexité de chacun. En effet, quelle donnée fournie dans le dossier peut fidèlement refléter la capacité d'une personne, après la perte d'un emploi, de s'adapter et trouver un nouvel emploi rapidement[1710] ? Une telle capacité, importante dans la détermination d'un taux d'assurance, se révèle difficile à traduire en données. Le caractère indulgent de la CNIL à l'égard de ces décisions doit donc être critiqué, notamment parce qu'il va à l'encontre de la volonté du législateur.

L'étude des arrêts des juridictions administratives confirme la fonction plutôt symbolique de l'ancien article 10 de la loi Informatique et libertés. À l'instar de la CNIL, les juges administratifs avaient du mal à reconnaître qu'une décision pouvait être prise sur le seul fondement d'un traitement automatisé[1711].

[1707] V. sur cette question : *JCl. comm.,* fasc. 940, « Données à caractère personnel. Obligations des personnes mettant en œuvre des traitements de données à caractère personnel et droits des personnes concernées », par R. Perray, 2016 (actu. 2020), nos 73 s. ; A. Türk, « Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », Sénat, no 218, 19 mars 2003, p. 67.

[1708] A. Debet, « APB enfin remis en cause par la CNIL », *CCE* 2017, no 12, comm. 101.

[1709] M. Gaudemet et R. Perray, « "Scoring" et protection des données personnelles : un nouveau régime à l'efficacité incertaine », *LPA* 30 mai 2006, no 107, p. 8.

[1710] A. Rouvroy, « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data », in Conseil d'État, « Le numérique et les droits fondamentaux », *Rapport Public 2014*, La Documentation française, 2014, p. 416.

[1711] V. par ex. CAA Nantes, 25 mars 2011, no 10NT02172, inédit *Lebon*, ou CCA Douai, 19 juin 2008, no 07DA00077, inédit *Lebon*. Sur cette question, v. A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, no 853, p. 342. Le juge judiciaire a été relativement épargné par ces questions puisque très peu de ses décisions sont fondées sur cet article. Pour un exemple, v. Cass. crim., 5 avr. 2006, no 04-87.504, *NPB*.

Les dispositions du règlement reprennent les principes de la directive, tout en essayant de répondre aux risques identifiés pour le profilage.

452. Le champ circonscrit des décisions individuelles automatisées dans le règlement européen. Le règlement européen reprend, dans son article 22, le principe selon lequel la personne « a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé ». Le terme « droit » pourrait laisser penser que seul un refus explicite de la personne permettrait d'échapper à ces décisions. Fort heureusement, le G29 a précisé que l'article 22 du règlement européen établissait une *interdiction générale* de prendre des décisions fondées exclusivement sur un traitement automatisé, et cela, quelle que soit l'attitude de la personne concernée[1712]. Face à cette interdiction, des auteurs se sont demandés s'il n'était pas possible de qualifier ce droit comme un droit subjectif de tout individu à ne pas faire l'objet d'une décision exclusivement fondée sur un traitement automatisé[1713]. La réalité actuelle des traitements de données laisse peu d'espoir pour une telle consécration, autrement que symbolique. En tout état de cause, si un tel droit existait, il aurait un champ d'application très réduit. En effet, pour qu'une telle interdiction s'applique, deux conditions cumulatives doivent être remplies : d'une part, la prise de décision doit reposer *exclusivement* sur un traitement automatisé[1714] et d'autre part, elle doit produire des *effets juridiques* pour la personne concernée ou des *effets similaires* l'affectant de manière significative. L'étendue de ce qui affecte une personne « de manière significative » est difficile à déterminer et relève nécessairement d'une application *in concreto* difficile à prédire[1715].

Pour le G29, le niveau d'importance de la décision affectant la personne de manière significative doit être similaire à celui d'une décision produisant un effet juridique, mais surtout les effets de cette décision doivent être suffisamment

---

[1712] G29, WP 251 rév. 01, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, 6 févr. 2018, p. 21.
[1713] N. Martial-Braz, « L'abus de textes peut-il nuire à l'efficacité du droit ? La théorie du mille-feuille législatif à l'épreuve de la protection des données à caractère personnel », *Dalloz IP/IT* 2018, p. 459 ; L. Cluzel-Métayer et E. Debaets, « Le droit de la protection des données personnelles : la loi du 20 juin 2018 », *RFDA* 2018, p. 1101 ; N. Martial-Braz et J. Rochfeld (dir.), *Droit des données personnelles. Les spécificités du droit français au regard du RGPD*, Dalloz, 2019, nº 1107, p. 181 s.
[1714] Si le traitement fait l'objet d'une intervention humaine, la première condition ne sera pas remplie. Toutefois, cette intervention humaine ne doit pas être insignifiante ou artificielle, v. N. Martial-Braz, « Le profilage. Fiche pratique », *CCE* 2018, nº 4, comm. 15. V. aussi, G29, WP 251 rév. 01, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, 6 févr. 2018, p. 23.
[1715] N. Martial-Braz, « Le profilage. Fiche pratique », *CCE* 2018, nº 4, comm. 15 ; J. Rochfeld, « L'encadrement des décisions prises par algorithme », *Dalloz IP/IT* 2018, p. 474.

conséquents ou importants[1716]. Ainsi, seules les décisions dont les effets sont les plus graves sont concernées par l'article 22 du règlement européen. Le champ de l'interdiction est donc très réduit[1717].

Trois exceptions viennent encore empiéter sur ce principe puisque les décisions fondées sur un traitement automatisé de données restent possibles si elles sont liées à la conclusion ou à l'exécution d'un contrat ; si elles sont prévues par le droit national ou européen ; ou si la personne concernée y a explicitement consenti[1718]. Pour pouvoir invoquer l'une de ces trois exceptions, le responsable du traitement doit tout de même employer des mesures appropriées pour garantir les droits et les intérêts légitimes de la personne concernée[1719].

Le champ d'application réduit de l'interdiction, cumulé à ces trois exceptions, amène à s'interroger sur la portée exacte de l'article 22 du règlement[1720]. D'autant que, malgré une volonté affichée d'encadrer le profilage, cet article s'applique uniquement aux profilages les *plus intrusifs*[1721]. À ces éléments s'ajoute également une implémentation particulière de ce dispositif en droit français[1722].

453. Les spécificités du droit français. En dépit de la marge de manœuvre relativement circonscrite octroyée par l'article 22 du règlement européen, le législateur français a proposé un dispositif particulier. Il a repris, assez maladroitement, certaines des dispositions de cet article, tout en modifiant parfois leur sens et leur portée. Ainsi, l'article 47 de la loi Informatique et libertés prévoit une interdiction de principe des décisions fondées uniquement sur un traitement automatisé de données, là où

[1716] G29, WP 251 rév. 01, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, 6 févr. 2018, p. 23 s. Pour une discussion sur la signification concrète de ces notions, v. not. J. Rochfeld, « L'encadrement des décisions prises par algorithme », *Dalloz IP/IT* 2018, p. 474.
[1717] Les exemples fournis par le G29 confirment cette impression d'application très réduite du principe d'interdiction puisque le groupement considère que peuvent entrer dans cette catégorie les décisions ayant une incidence sur la situation financière d'une personne, affectant l'accès aux services de santé, ou à l'éduction, v. G29, WP 251 rév. 01, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, 6 févr. 2018, p. 24.
[1718] Art. 22 § 2 du règlement UE nº 2016/679.
[1719] Art. 22 § 3 du règlement UE nº 2016/679.
[1720] La CNIL se demande d'ailleurs si ces exceptions ne vident pas de sa substance le principe d'interdiction des décisions fondées sur un traitement automatisé de données personnelles, v. CNIL, « Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle », Rapport de synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une République numérique, déc. 2017, p. 52. V. aussi, S. Wachter, B. Mittlestadt et L. Floridi, « Why a right to explanation of automated decision-making does not exist in the general data protection regulation », *International Data Privacy Law* 2017, vol. 7, p. 76 s.
[1721] Seuls les traitements qui reposent sur un traitement automatisé impliquant une prise de décision automatisée et qui produisent des effets juridiques concernant la personne ou qui l'affecte de manière significative de façon similaire sont concernés, v. N. Martial-Braz, « Le profilage. Fiche pratique », *CCE* 2018, nº 4, comm. 15, § 4.
[1722] Sur la mise en œuvre de la marge d'action française, v. not. J. Rochfeld, « L'encadrement des décisions prises par algorithme », *Dalloz IP/IT* 2018, p. 474.

l'article 22 du règlement européen édicte une forme de droit subjectif[1723]. Par ailleurs, la loi française réduit le domaine de l'interdiction puisque ce sont les décisions produisant des effets juridiques à l'égard d'une personne ou celles « l'affectant de manière significative » qui sont désormais visées[1724]. Quant aux exceptions, l'article 47 de la loi Informatique et libertés opère un renvoi au droit européen, tout en ajoutant la possibilité, pour les personnes concernées, d'accéder aux « règles définissant le traitement ainsi que les principales caractéristiques de sa mise en œuvre »[1725]. Si une opinion doctrinale considère que cet article encadre mieux les pratiques liées aux traitements automatisés de données[1726], d'autres auteurs n'ont pas manqué de relever les incohérences que l'implémentation française génère[1727].

Ainsi, les principes juridiques applicables aux prises de décisions fondées sur des traitements automatisés de données ont un champ d'application très réduit : ils s'appliquent aux décisions les plus intrusives et n'encadrent pas la plupart des autres décisions. En conséquence, un grand nombre de décisions n'entrent pas dans les catégories édifiées par les législateurs. Pourtant, elles comportent des risques importants pour les personnes.

B. Les risques liés aux décisions fondées sur un traitement automatisé

454. Constat. Plus de quatre décennies nous séparent des premières mesures législatives encadrant les décisions prises sur le fondement de traitements automatisés de données. La mise en œuvre de ces principes semble contestable tant les décisions

---

[1723] Cet article a été soumis à l'examen du Conseil constitutionnel qui a validé la possibilité d'avoir recours aux algorithmes décisionnels, tout en déduisant de l'obligation de transparence une prohibition de principe « des algorithmes susceptibles de réviser eux-mêmes les règles qu'ils appliquent, sans le contrôle et la validation du responsable du traitement ». Plus précisément, le Conseil constitutionnel a considéré que l'administration devait respecter plusieurs conditions pour pouvoir prendre des décisions fondées sur un traitement automatisé de données : elle doit être en mesure de communiquer, à la demande de la personne concernée, les principales caractéristiques de mise en œuvre de l'algorithme ; la décision administrative doit pouvoir faire l'objet d'un recours administratif ; et le responsable du traitement doit toujours s'assurer de la maîtrise du traitement automatisé et de ses évolutions afin d'être en mesure d'expliquer en détail et sous une forme intelligible la mise en œuvre du traitement à l'égard de la personne concernée (empêchant ainsi le recours au *machine learning*), v. Cons. const., 12 juin 2018, n° 2018-765 DC, cons. 71. Pour une analyse de ces questions, v. not. A. Sée, « La régulation des algorithmes : un nouveau modèle de globalisation ? », *RFDA* 2019, p. 830.

[1724] N. Martial-Braz, « L'abus de textes peut-il nuire à l'efficacité du droit ? La théorie du mille-feuille législatif à l'épreuve de la protection des données à caractère personnel », *Dalloz IP/IT* 2018, p. 459.

[1725] D'ailleurs, il est possible de se demander comment ce droit d'accès s'articule avec l'obligation d'information préalable posée aux articles 13 et 14 du règlement européen. Sur ce point, v. J. Rochfeld, « L'encadrement des décisions prises par algorithme », *Dalloz IP/IT* 2018, p. 474.

[1726] B. Fauvarque-Cosson et W. Maxwell, « Protection des données personnelles », *D.* 2018, p. 1033.

[1727] N. Martial-Braz, « L'abus de textes peut-il nuire à l'efficacité du droit ? La théorie du mille-feuille législatif à l'épreuve de la protection des données à caractère personnel », *Dalloz IP/IT* 2018, p. 459 ; J. Rochfeld, « L'encadrement des décisions prises par algorithme », *Dalloz IP/IT* 2018, p. 474. Sur cette question, v. plus largement, N. Martial-Braz et J. Rochfeld (dir.), *Droit des données personnelles. Les spécificités du droit français au regard du RGPD*, Dalloz, 2019, n^os^ 1101 s., p. 174 s.

fondées sur ces traitements ont prospéré. Celles-ci se sont multipliées et banalisées et ont investi tous les domaines de notre société[1728]. Il est d'ailleurs possible de constater une confiance de l'utilisateur à l'égard de ces décisions, qui sont souvent perçues comme plus objectives[1729]. En effet, les personnes ont tendance à imaginer qu'un traitement effectué par une machine est plus objectif que celui effectué par un humain[1730].

Ainsi, les règles juridiques n'ont pas empêché le développement d'une société gouvernée par les nombres, les profils et la segmentation[1731]. N'est-il pas désormais évident de se laisser guider dans sa conduite par un traitement automatisé qui détermine les rues que l'on emprunte ? Et cela même si le chemin proposé est plus long puisque l'application utilisée fait également de la régulation de trafic[1732]. N'est-il pas classique d'obtenir des résultats de recherche personnalisés *via* les moteurs de recherche ou de se voir recommander un film en fonction des films déjà visionnés[1733] ? Aucun de ces traitements n'entre dans le champ d'application de l'article 22 du règlement européen puisqu'ils ne prennent pas une décision produisant d'effet juridique ou affectant la personne de manière significative. Pourtant, ces petites décisions ont un impact d'ensemble important sur le développement des opinions et sur l'autonomie personnelle. En effet, n'est-il pas culturellement marquant d'encourager les personnes à regarder certains films ou à lire certains livres ?

455. L'influence des traitements automatisés sur la liberté d'autodétermination. Les règles actuelles concernent les traitements automatisés dont les effets sont les plus redoutables. Pour autant, sans avoir de telles conséquences directes, certains

---

[1728] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 853, p. 342.

[1729] CNIL, « Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle », Rapport de synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une République numérique, déc. 2017, p. 40. V. aussi, A. Rouvroy, « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data », in Conseil d'État, « Le numérique et les droits fondamentaux », *Rapport Public 2014*, La Documentation française, 2014, p. 416.

[1730] Cette perception est fausse puisque le traitement automatisé dépend du code écrit par une personne et des donnée enregistrées.

[1731] A. Supiot, *La Gouvernance par les nombres. Cours au Collège de France (2012-2014)*, Fayard, 2015, p. 23 s. Le Rapport Tricot alertait déjà sur le renforcement de la « catégorisation des situations et des individus », B. Tricot, « Rapport de la commission Informatique et libertés », La Documentation française, 1975, p. 15.

[1732] A. Courmont, « Plateforme, *big data* et recomposition du gouvernement urbain : les effets de Waze sur les politiques de régulation du trafic », *Revue française de sociologie* 2018, vol. 59, p. 423. V. aussi D. Cardon et M. Crépel, « Les algorithmes et la régulation des territoires », in *Gouverner la ville numérique*, dir. A. Courmont et P. Le Galès, PUF, 2019.

[1733] Plus de 80 % du contenu regardé par les utilisateurs de Netflix proviennent du système de recommandation personnalisé, v. C. Gomez-Uribe et N. Hunt, « The Netflix recommender system : algorithms, business value, and innovation », *ACM Transactions on Management Information Systems* 2015, vol. 6, nº 4, article 13, p. 5.

traitements influencent, sur le long terme, le mode de pensée et risquent donc de porter atteinte à la liberté d'autodétermination. Par exemple, le moteur de recherche Google hiérarchise l'information proposée à un utilisateur grâce à de multiples critères personnalisés tels que la localisation, les précédentes recherches ou les sites visités[1734]. Sur Amazon, les algorithmes analysent les prédilections d'un acheteur pour ensuite lui soumettre des produits qui, compte tenu de leurs analyses, devraient le séduire. Sur Facebook, ce sont les interactions sociales qui sont inspectées pour décider notamment des suggestions d'amis et des publicités proposées[1735]. À force d'être épiées, profilées et orientées, les personnes perdent progressivement leur capacité à se déterminer librement.

La notion de « *filter bubble* » proposée par Monsieur Eli Pariser illustre ce mouvement enfermant les personnes dans des traitements algorithmiques, dont le but est de filtrer les informations auxquelles elles sont exposées pour certaines finalités extérieures à la personne[1736]. En enfermant les personnes dans leur « bulle », les traitements modifient la perception de ce qu'est la « réalité »[1737] et empêche les utilisateurs d'être confrontés à des idées, des intérêts ou des préférences différents de ceux qu'ils ont habituellement[1738]. Des chercheurs montrent même qu'un individu moyen n'adapte ses jugements que si les opinions auxquelles il est confronté n'en sont pas trop éloignées : si elles le sont, la personne ne va même pas lui accorder son attention[1739]. L'impact de ces bulles filtrantes a déjà montré ses effets, notamment à

[1734] Selon certaines études, Google utiliserait plusieurs dizaines de signaux pour personnaliser les résultats, v. E. Pariser, *The filter bubble,* Penguin Press, 2011, p. 6 ; J. Grimmelmann, « The structure of search engine law », *Iowa Law Review* 2007, vol. 93, p. 1 s. [93 IOWA. L. REV. 1], spéc. p. 15. Sur l'impact des moteurs de recherche dans l'accès à l'information, v. par ex., L. Introna et H. Nissenbaum, « Shaping the Web : why the politics of search engines matters », *The Information society* 2000, vol. 16, p. 1 et E. Van Couvering, *Search engine bias. The structuration of traffic on the World-Wide Web*, th. London School of Economics and Political Science, 2009, p. 15.

[1735] C. Hildebrand et T. Schlager, « Focusing on others before you shop : exposure to Facebook promotes conventional product configurations », *Journal of the Academy of Marketing Science* 2019, vol. 47, p. 291 s. [47 J. OF THE ACAD. MARK. SCI. 291].

[1736] E. Pariser, *The filter bubble,* Penguin Press, 2011, p. 6. Pour une critique de ce concept, v. not. T. Nguyen, P.-M. Hui, F. Harper, L. Terveen et J. Konstan, « Exploring the filter bubble : the effect of using recommender systems on content diversity », *WWW* 2014, p. 677 ; M. Haim, A. Graefe et H.-B. Brosius, « Burst of the filter bubble ? Effects of personalization on the diversity of Google News », *Digital Journalism* 2016, vol. 6, nº 3, p. 330.

[1737] P. de Filippi, « Gouvernance algorithmique : vie privée et autonomie individuelle à l'ère des *Big Data* », in *Open data & data protection : nouveaux défis pour la vie privée*, dir. D. Bourcier et P. de Filippi, Mare & Martin, 2016.

[1738] E. Pariser, « When the Internet thinks it knows you », *The New York Times* 22 mai 2011.

[1739] G. Deffuant, D. Neau, F. Amblard et G. Weisbuch, « Mixing Beliefs among Interacting Agents », *Advances in Complex Systems* 2000, vol. 3, nº 1, p. 87 s.

l'occasion de la campagne électorale de 2016 de Donald Trump[1740] ou dans le développement de désinformation[1741].

En sus, des études montrent que les algorithmes de recommandation font plus qu'inciter les utilisateurs à consommer de nouveaux produits ou services, ils *façonnent* leurs goûts et leurs préférences[1742]. Pour le philosophe Benjamin Curtis, cette personnalisation érode notre capacité à penser librement[1743]. Plus spécifiquement, notre libre arbitre est prédit et influencé par nos précédentes traces et par le passé de ceux qui nous ressemblent[1744]. Il est sans doute excessif de dire que ces algorithmes nous contrôlent, mais ils orientent assurément nombre de nos décisions : du choix d'un hôtel ou d'un billet d'avion à celui d'un itinéraire, de l'achat d'un livre sur Internet à la rencontre amoureuse sur l'application de rencontres en passant par notre vote pour un candidat aux élections, les algorithmes influencent la plupart de nos décisions[1745]. Ces pratiques n'ont pas seulement des effets sur les personnes prises individuellement puisqu'elles engendrent également des conséquences sur la société dans son ensemble.

456. L'influence des traitements automatisés sur la société. À force de catégoriser, profiler et effacer les nuances propres à chaque personne, les algorithmes tendent à normaliser notre société. Dans cette société normalisée, il est de plus en plus difficile d'être soi-même sans ressembler aux autres. La société dans son ensemble risque donc de perdre en nuances, et un préjudice collectif pourrait résulter de la diffusion de ces traitements automatisés[1746].

En plus de ces risques de normalisation de la société, certains algorithmes renforcent les biais et engendrent des discriminations. À ce titre, les algorithmes d'apprentissage font peser des menaces renouvelées pour les minorités et l'ensemble de la société[1747]. L'algorithme utilisé par Amazon pour classer les nouvelles

---

[1740] D. Baer, « The "filter bubble" explains why Trump won and you didn't see it coming », *The Cut* 9 nov. 2016.
[1741] J. Kelly et C. François, « This is what filter bubbles actually look like. Maps of Twitter activity show how political polarization manifests only and why divides are so hard to bridge », *MIT Tech Review* 2018, vol. 121.
[1742] G. Adomavicius, J. Bockstedt, S. Curley et J. Zhang, « Effects of online recommendations on consumers' willingness to pay », *Management Science* 2017, vol. 64, nº 11 et G. Adomavicius, J. Bockstedt, S. Curley, J. Zhang et S. Ransbotham, « The hidden side effects of recommendation systems », *MIT Sloan Management Review* 2019, p. 19 s.
[1743] B. Curtis, « Google at 20 : how a search engine became a literal extension of our mind », *The Conversation* 3 sept. 2018.
[1744] D. Cardon, *À quoi rêvent les algorithmes : nos vies à l'heure des big data,* Seuil, 2015, p. 34.
[1745] J. Béranger, « Big data et données personnelles : vers une gouvernance ethnique des algorithmes », *ParisTech Review* 22 déc. 2014.
[1746] Sur la reconnaissance d'un tel préjudice, v. *infra*, nº 579.
[1747] Défenseur des droits et CNIL, « Algorithmes : prévenir l'automatisation des discriminations », 2020. V. aussi, S. Merabet, *Vers un droit de l'intelligence artificielle,* th. Aix-Marseille, 2018, Dalloz, nº 250, p. 242.

candidatures en fonction des *curriculum vitae* de ses employés illustre bien ces enjeux[1748]. En pratique, cet algorithme attribuait fréquemment de mauvaises notes aux profils de femmes et favorisait certains mots, plus présents dans les *curriculum vitae* masculins. Un tel déséquilibre s'expliquait par le manque de représentativité des données fournies en entrée, dans lesquelles les hommes constituaient l'écrasante majorité des cadres recrutés par le passé. En reproduisant les choix passés, l'algorithme ne laissait aucune chance aux candidatures féminines.

Les algorithmes d'apprentissage risquent donc de perpétuer les biais présents dans les données d'entraînement et d'engendrer des discriminations[1749]. Le droit des données personnelles devrait s'ériger comme un rempart contre ces risques.

C. La consolidation des règles entourant les décisions fondées sur un traitement automatisé

457. Renforcement de certains principes. Dans son rapport sur l'intelligence artificielle, la CNIL appelait au renforcement du principe de loyauté et de celui de vigilance[1750]. Ces deux principes sont effectivement essentiels dans le développement d'algorithmes qui respectent les personnes.

458. Le renforcement du principe de loyauté. Le principe de loyauté, entendu comme le système qui « consiste à assurer de bonne foi le service de classement ou de référencement, sans chercher à l'altérer ou à le détourner à des fins étrangères à l'intérêt des utilisateurs »[1751], encadre la liberté du responsable du traitement dans les critères de fonctionnement de l'algorithme. Le responsable du traitement doit alors mettre au cœur des choix de son algorithme l'intérêt des utilisateurs et faire prévaloir les intérêts collectifs (c'est-à-dire les intérêts des utilisateurs et de la société devant ses propres intérêts)[1752]. Il vise donc à s'assurer que l'exécution de l'algorithme reste conforme aux

---

[1748] J. Dastin, « Amazon scraps secret AI recruiting tool that showed bias against women », *Reuters* 10 oct. 2018.
[1749] Sur un panorama complet des enjeux liés aux algorithmes, v. P. Bertail, D. Bounie, S. Clémençon et P. Waelbroeck, « Algorithmes : biais, discrimination et équité », *Télécom ParisTech* févr. 2019. Plus généralement sur les interactions entre les discriminations et la vie privée, v. B. Beignier, « Rapport Français », in *Travaux de l'Association Henri Capitant*, « La discrimination », t. 51, Journées franco-belges, SLC, 2004, p. 604 s.
[1750] CNIL, « Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle », Rapport de synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une République numérique, déc. 2017, p. 48.
[1751] Conseil d'État, « Le numérique et les droits fondamentaux », *Rapport Public 2014*, La Documentation française, 2014, p. 273 et 278 s.
[1752] CNIL, « Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle », Rapport de synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une République numérique, déc. 2017, p. 49.

prévisions mais aussi à vérifier que l'intérêt qui prime est celui collectif. Un tel principe semble capital pour assurer une mise en œuvre respectueuse des personnes. La loyauté instille donc une double exigence : elle renvoie à une obligation négative de ne pas abuser de la confiance accordée tout en traduisant une obligation positive d'adopter une attitude exemplaire[1753]. Ainsi, la loyauté a nécessairement un caractère subjectif lequel appelle au renforcement des contrôles. Ces contrôles ne peuvent se limiter aux opérations ponctuelles menées par la CNIL, mais doivent inclure un renforcement du principe de vigilance. Cela passe notamment par une plus grande responsabilisation des personnes qui travaillent sur ces algorithmes prédictifs[1754].

459. Le renforcement du principe de vigilance. Le principe de vigilance se résume à un principe méthodologique orientant la façon dont sont définis les systèmes algorithmiques[1755]. Ce principe est nécessaire notamment pour encadrer les algorithmes d'apprentissage automatique qui sont, par nature, mouvants et évolutifs. Il a vocation à s'appliquer à l'ensemble des personnes impliquées dans la chaîne algorithmique (le développeur, la personne collectant les données, le *data scientist*, l'utilisateur final…). Sa mise en œuvre garantit une pluralité de garde-fous tant que chaque personne impliquée a non seulement le pouvoir effectif de vérifier l'exécution de l'algorithme, mais surtout la possibilité de s'assurer qu'il est conforme aux principes annoncés[1756].

460. Diversification des contrôles. Les recommandations encourageant une responsabilité individuelle des personnes impliquées dans la chaîne algorithmique illustrent les lacunes du système actuel reposant sur des contrôles centralisés et en silos. Pour garantir le respect du droit des données personnelles, il faut donc non seulement augmenter les contrôles opérés par les institutions de contrôle classiques, mais aussi diversifier ces contrôles et favoriser les contrôles internes aux organismes. Ces contrôles ne peuvent être efficaces que si la culture de la protection des données y est considérée comme l'une des priorités lors de la mise en œuvre des traitements.

[1753] Sur la double signification de la loyauté, v. not. D. Mongoin, « Rapport introductif », in *La loyauté en droit public,* dir. S. Hourson et S. Ferrari, Institut universitaire Varenne, 2018, p. 21 s., spéc. p. 32 s.
[1754] V. *infra*, n^os^ 499 s.
[1755] CNIL, « Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle », Rapport de synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une République numérique, déc. 2017, p. 50.
[1756] Sur la responsabilité de ces personnes, v. *infra*, n^os^ 499 s.

461. Conclusion de chapitre. Le droit des données à caractère personnel prévoit plusieurs principes importants pour la protection des personnes. Pour autant, certaines améliorations sont utiles pour rendre ces principes plus efficaces.

Un mouvement d'encadrement de certains pouvoirs a donc été proposé, notamment pour le droit à l'oubli et les principes relatifs aux accès aux données. Pour le premier, l'application étendue du droit à l'oubli s'est révélée engendrer plusieurs externalités négatives, notamment sur la liberté d'expression. Plutôt que de consacrer un principe de droit à l'oubli, il vaudrait mieux garantir une application irréprochable des principes de licéité des données personnelles et limiter l'effacement aux publications illicites. Par ailleurs, seul le juge devrait être compétent pour mettre en balance des libertés individuelles et juger quel intérêt est le plus légitime. Dans le second cas, c'est-à-dire en ce qui concerne les accès aux données personnelles par des tiers, les règles actuelles sont trop permissives. Pour renforcer la prérogative de contrôle des personnes concernées à l'égard de leurs données personnelles, il semble donc nécessaire d'encadrer les situations dans lesquelles ces données peuvent être communiquées. Un principe de non-transmission doit ainsi être affirmé, et seul le consentement de la personne, au sens du droit des données à caractère personnel, devrait rendre licite cette transmission.

À l'inverse, d'autres principes de protection des données personnelles doivent être raffermis. Il s'agit d'abord du principe de minimisation qui évite, en théorie, une collecte trop large des données. La consolidation de ce principe passe par une application stricte des règles de proportionnalité et par une augmentation des contrôles. Enfin, les règles encadrant les prises de décisions automatisées devraient elles aussi être renforcées, notamment avec la consolidation des principes de loyauté et de vigilance et grâce à une diversification des contrôles.

462. Conclusion de titre. Le droit des données personnelles préserve plusieurs intérêts : ce droit favorise les traitements de données, notamment pour valoriser le développement de l'informatique mais il vise aussi à protéger les personnes contre les effets des traitements. L'équilibre entre ces intérêts est délicat, à trouver et il est apparu que des principes devaient être renforcés pour garantir une meilleure protection des personnes. Ces renforcements doivent être conduits à la lumière des prérogatives garanties par le droit des données personnelles, c'est-à-dire le contrôle des personnes à l'égard de leurs données et leur liberté d'autodétermination. Cette dernière est

essentielle pour assurer aux personnes un développement autonome de leur personnalité et réduire les influences extérieures prolongées qui peuvent la manipuler. Les évolutions proposées visent à renforcer ces deux prérogatives.

La plupart des principes du droit des données personnelles montrent toutefois une faiblesse commune : celle d'une mise en œuvre disparate, notamment liée à l'insuffisance des contrôles et à l'absence de mesures sanctionnant les manquements. Seul un meilleur respect de ces règles permettra d'assurer une protection effective des personnes. Cette amélioration passe par une amélioration de la mise en œuvre du droit des données à caractère personnel.

TITRE II – AMÉLIORER LA MISE EN ŒUVRE DU DROIT DES DONNÉES À CARACTÈRE PERSONNEL

463. Garantir une meilleure mise en œuvre des principes. Plus de quatre décennies se sont écoulées depuis l'adoption des premières règles encadrant les traitements de données personnelles. Les évolutions successives de ce droit lui ont permis de s'adapter pour préserver l'équilibre entre protection des personnes et permission des traitements. De nombreux auteurs regrettent toutefois que l'effectivité de cette matière ne soit pas toujours garantie, notamment du fait de divergences fondamentales entre la lettre des textes et la réalité des traitements[1757]. Ces auteurs regrettent que beaucoup des principes du droit des données personnelles restent lettre morte. Il est vrai que les meilleures règles sont peu de chose lorsqu'elles ne sont pas assorties de moyens de les mettre en œuvre[1758]. Ainsi, l'une des difficultés de cette matière est celle liée à l'application concrète de ses principes. Garantir une telle mise en œuvre est d'autant plus complexe que les traitements de données sont plus que jamais ancrés dans notre quotidien. Les personnes sont constamment sommées de fournir des données et sont soumises à des traitements dont elles ne réalisent pas toujours l'ampleur ni l'impact. Face à ces sollicitations, les personnes concernées se sentent souvent abandonnées, démunies et non protégées[1759]. Comment leur attribuer un réel pouvoir à l'égard de leurs données ? À plusieurs reprises, l'importance de la mise en œuvre des principes et des contrôles s'est manifestée. Pour garantir cette mise en œuvre une pluralité d'acteurs sont mobilisés.

464. Un cumul d'acteurs impliqués dans la mise en œuvre du droit des données à caractère personnel. Plusieurs types d'acteurs interviennent dans la mise en œuvre

---

[1757] B.-J. Koops, « The trouble with European data protection law », *International Data Privacy Law* 2014, vol. 4, p. 250 s.
[1758] D. Cohen, « Le juge, gardien des libertés ? », *Pouvoirs* 2009, nº 130, p. 113.
[1759] C'est ce que certains auteurs qualifient de *privacy nihilism*, v. I. Bogost, « Welcome to the age of privacy nihilism », *The Atlantic* 23 août 2018. Le concept de paradoxe de la vie privée (*privacy paradox*) peut également expliquer ces comportements. En effet, cette expression est souvent employée pour « désigner le fait que les individus se montrent, dans les enquêtes d'opinion, inquiets de la diffusion de leurs données personnelles mais ne modifient pas leur comportement. Ce paradoxe s'explique peut-être par le fait que les individus perçoivent mal les risques concrets associés à cette diffusion », L. Cytermann, « La loi Informatique et libertés est-elle dépassée ? », *RFDA* 2015, p. 99. Pour des développements plus conséquents sur ce sujet, v. D. Solove, « The myth of the privacy paradox », *George Washington Law Review* 2021, vol. 89 [89 GEO. WASH. L. REV.].

de la protection des personnes. La CNIL est l'institution désignée par le droit des données à caractère personnel pour en surveiller l'application[1760]. Elle occupe donc une place capitale dans la mise en œuvre de cette matière. Les pouvoirs qui lui sont octroyés sont larges et ne cessent d'augmenter. D'autres acteurs spécialisés l'accompagnent dans cette mission et participent à une mise en œuvre effective de la protection au sein des organismes. D'autres formes de contrôles spécialisés ne sont-elles pas envisageables ? En sus de ces acteurs spécialisés, quelle est la place des acteurs du droit commun dans la mise en œuvre de la matière ? À première vue, il apparaît que les juridictions ne sont guère sollicitées par les plaignants dans cette matière. Pourtant, la sanction du droit est souvent présentée comme la condition de son efficacité[1761]. Dès lors, la réalisation juridictionnelle se révèle essentielle à l'efficacité du droit des données à caractère personnel.

465. Plan. L'étude des contrôles des acteurs spécialisés (Chapitre I) précèdera l'analyse de sa réalisation juridictionnelle (Chapitre II).

[1760] Art. 51 § 1 du règlement UE nº 2016/679 et art. 8 de la loi nº 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018.
[1761] P. Malinvaud, *Introduction à l'étude du droit*, 20e éd., LexisNexis, 2020, nº 479, p. 434.

Chapitre I – Les contrôles des acteurs spécialisés

466. L'autorité administrative, point cardinal de la mise en œuvre du droit des données personnelles. Depuis ses premières règles, le législateur français a placé la CNIL au cœur de la mise en œuvre du droit des données personnelles. L'institution recevait les formalités déclaratives, autorisait les traitements, informait les responsables du traitement, assistait les personnes concernées… En plus de ces missions, le législateur lui a confié en 2004 des pouvoirs de contrôle[1762] et de sanction[1763]. Sans doute l'autorité était-elle considérée comme la mieux placée pour garantir le respect de ce droit de « spécialistes ». Cet empilement des pouvoirs confiés à la CNIL amène à s'interroger sur les garanties que cette dernière présente. En effet, « une grande responsabilité est la suite inséparable d'un grand pouvoir »[1764]. Et donc, les garanties présentées par la CNIL sont-elles suffisantes par rapport à ses nombreux pouvoirs ?

467. Les autres acteurs. Longtemps, la CNIL a été perçue comme le meilleur acteur pour garantir la mise en œuvre du droit. Pour autant, la centralisation des pouvoirs de contrôle a montré certaines limites. Lenteur dans le traitement des demandes, choix des dossiers, faibles moyens, sont quelques-unes des limites auxquelles l'action de la CNIL est confrontée. Dès lors, les contrôles ne devraient-ils pas être diversifiés pour mieux diffuser la culture de la protection des données ?

468. Plan. Face aux nombreux pouvoirs de la CNIL, l'institution se doit d'être exemplaire et son activité doit faire l'objet d'un examen minutieux. Aux contrôles sur la CNIL (Section I) s'ajoute aussi l'importance des contrôles effectués par les autres acteurs spécialisés (Section II).

SECTION I – LES CONTRÔLES SUR LA CNIL

469. Les spécificités des autorités de contrôle. La variété des missions des autorités de contrôle les oblige à présenter des garanties particulières. Ces institutions doivent

[1762] Art. 44 de la loi n° 78-17 du 6 janv. 1978 telle que modifiée par la loi n° 2004-801 du 6 août 2004.
[1763] Art. 45 s. de la loi n° 78-17 du 6 janv. 1978 telle que modifiée par la loi n° 2004-801 du 6 août 2004.
[1764] Convention Nationale, *Archives parlementaires*, série 1, t. 64, 7 mai 1793, p. 287.

être indépendantes, tout en ayant une prise sur la réalité des traitements, et elles doivent être spécialisées tout en étant transdisciplinaires. L'indépendance des autorités est-elle garantie à tous les niveaux ? Les garanties procédurales ont-elles été adaptées aux nouvelles missions contentieuses de l'autorité ?

470. Plan. Le système de contrôle instauré par le droit des données personnelles requiert un renforcement des garanties d'indépendance de la CNIL (§ I), des garanties procédurales devant l'institution (§ II) ainsi qu'une mixité de profils en son sein (§ III).

§ I. Renforcer les garanties d'indépendance de la CNIL

471. Les autorités administratives indépendantes. L'une des innovations de la loi du 6 janvier 1978 a été d'instaurer la première autorité administrative indépendante en France[1765]. Selon une définition couramment admise, les autorités administratives indépendantes agissent au nom de l'État sans être subordonnées au gouvernement, et bénéficient, pour le bon exercice de leurs missions, de garanties leur accordant une pleine autonomie, évitant ainsi que leur action soit orientée ou censurée, si ce n'est par un juge[1766]. Face à la diversité des missions qui sont confiées à ces autorités, les pouvoirs dont elles sont dotées sont très hétérogènes dans leur nature et leur étendue. Ils vont du pouvoir consultatif au pouvoir de sanction, en passant par l'édiction de mesures règlementaires, ainsi que des pouvoirs d'autorisation, d'investigation et d'injonction[1767]. Les moyens mis à disposition de ces autorités varient en fonction de la diversité de leurs missions. À titre illustratif, en 2019, l'Autorité de la concurrence était dotée d'un budget annuel de 22,5 millions d'euros[1768] et la CNIL bénéficiait, quant à elle, d'un budget de 18,5 millions d'euros[1769]. Le domaine de compétence de la CNIL est pourtant plus large que celui de l'Autorité de la concurrence. En effet, la CNIL est le régulateur du droit des données personnelles ; elle contrôle sa bonne application non

[1765] Certains auteurs considèrent toutefois que la première autorité administrative indépendante n'est pas la CNIL mais la Commission des Opérations de Bourse créée en 1967, v. M.-A. Frison-Roche, « Autorités administratives incomprises (AAI) », *JCP G* 2010, nº 48, p. 1166.
[1766] Conseil d'État, « Les autorités administratives indépendantes », *Rapport Public 2001*, La Documentation française, 2001, p. 257.
[1767] Conseil d'État, « Les autorités administratives indépendantes », *Rapport Public 2001*, La Documentation française, 2001, p. 308.
[1768] En 2019, le budget de l'Autorité de la concurrence s'élevait à 22,53 millions d'euros. Dans ce montant, 17,23 millions d'euros étaient destinés aux dépenses de personnel et 5,3 millions d'euros étaient dédiés aux dépenses de fonctionnement et d'investissement, v. Autorité de la concurrence, *Rapport annuel 2019,* La Documentation française, p. 40.
[1769] CNIL, *Rapport d'activité 2019,* La Documentation française, 2020, p. 3.

seulement par les organismes du secteur public mais aussi ceux du secteur privé, et cela, quelle que soit leur taille. En comparaison, le domaine d'action de l'Autorité de la concurrence est plus réduit puisqu'elle ne s'intéresse qu'à la compétitivité et à la protection des consommateurs.

472. L'organisation de la CNIL. La CNIL est composée d'un collège de dix-huit membres nommés pour cinq années, et de plusieurs services organisés autour de directions, employant plus de deux cents agents. Depuis sa création en 1978, sa composition et les pouvoirs de ses services ont largement évolué. Les agents occupent désormais une place centrale dans l'activité de la Commission.

Le président de l'institution est nommé parmi les membres du collège par le président de la République[1770]. La Commission élit deux vice-présidents qui composent, avec son président, le bureau[1771]. Elle désigne une formation restreinte composée de cinq membres et d'un président (distinct du président de la CNIL)[1772]. Le pouvoir de prononcer des mesures coercitives et des sanctions est réparti entre le président de la CNIL et la formation restreinte[1773].

473. Plan. La variété des missions de l'autorité amène à s'interroger sur les garanties mises en place au sein du collège de la CNIL (A), ainsi que dans ses services (B) propres à garantir son indépendance et le bon emploi de ses ressources.

A. Les fortes garanties d'indépendance du collège de la CNIL

474. Garanties d'indépendance. Le rapport Tricot rappelait la nécessité pour l'autorité de jouir « d'une grande indépendance juridique et morale »[1774]. Le système a donc été construit pour garantir l'indépendance de l'autorité administrative. L'indépendance se définit classiquement comme l'absence de dépendance à l'égard d'un pouvoir extérieur[1775]. Elle doit exister vis-à-vis des milieux professionnels que

---

[1770] Art. 9 de la loi nº 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018.
[1771] Art. 9 de la loi nº 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018.
[1772] Art. 9 de la loi nº 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018.
[1773] Art. 16 et 20 de la loi nº 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018.
[1774] B. Tricot, « Rapport de la commission Informatique et libertés », La Documentation française, 1975, p. 74.
[1775] Monsieur Nino Longobardi définit l'indépendance comme « la non-dépendance vis-à-vis de manifestations de volonté d'autrui dans l'exercice de l'activité (d'instruction, d'information, de proposition, de consultation, de décision ou de jugement) déléguée à l'organisme », v. N. Longobardi, « Les autorités administratives indépendantes, une première approche (1re partie) », *LPA* 6 oct. 1995, nº 120, p. 4, spéc. p. 8.

l'institution contrôle, mais aussi à l'égard de l'État[1776]. Elle est donc centrale puisque l'autorité doit inspirer confiance et autorité[1777]. Cette indépendance se manifeste à plusieurs niveaux. Elle est d'abord historique et structurelle puisque depuis son origine, la loi du 6 janvier 1978 qualifie la CNIL d'« autorité administrative indépendante »[1778]. Ensuite, elle est organique, comme l'illustre la méthode de nomination de ses membres désignés par huit institutions différentes[1779]. Elle se manifeste enfin dans le statut personnel des membres du collège qui sont irrévocables[1780] et sont soumis à un régime strict d'incompatibilité[1781]. En dédiant une section entière à l'indépendance des autorités de contrôle et de leurs membres, le règlement européen conforte son importance[1782].

475. Une indépendance relative à l'égard du pouvoir politique. L'indépendance de la CNIL doit cependant être relativisée, notamment à l'égard du pouvoir politique, et ce pour au moins deux raisons. D'une part, la nomination des commissaires de la CNIL est le fait d'une discipline partisane inspirée par une stratégie politique. Ainsi, parmi les dix-huit commissaires, il est remarquable de noter que six d'entre eux sont désignés par le Parlement et trois par le gouvernement[1783]. La neutralité et l'impartialité de l'institution à l'égard du pouvoir politique sont discutables dès lors que ses membres doivent leur nomination à leur rôle dans la vie politique. D'ailleurs des auteurs n'ont pas manqué de relever quelques indices de l'influence du pouvoir politique sur les commissaires. En effet, il est arrivé que certains commissaires soutiennent des projets de loi du Gouvernement, y compris lorsque ce soutien contredisait la position officielle

---

[1776] A. Debet, « Autorités administratives indépendantes et personnalité morale », in *Travaux de l'Association Henri Capitant*, « La personnalité morale », t. 12, Journées nationales, Dalloz, 2010, p. 16.
[1777] L'une des raisons ayant justifié la création des autorités administratives indépendantes était celle du besoin d'offrir à l'opinion une garantie renforcée d'impartialité des interventions de l'État, v. Conseil d'État, « Les autorités administratives indépendantes », *Rapport Public 2001*, La Documentation française, 2001, p. 275.
[1778] Art. 8 de la loi nº 78-17 du 6 janv. 1978.
[1779] Art. 9 de la loi nº 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018.
[1780] La durée de leur mandat est, en principe, de cinq ans, mais pour les parlementaires, elle est égale à la durée de leur mandat électif, v. art. 9 de la loi nº 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018. La CJUE a ainsi considéré que « L'exigence d'indépendance figurant à l'article 28, paragraphe 1, second alinéa, de la directive 95/46 doit, dès lors, nécessairement être interprétée comme incluant l'obligation de respecter la durée du mandat des autorités de contrôle jusqu'à son échéance et de n'y mettre fin de manière anticipée que dans le respect des règles et des garanties de la législation applicable », v. CJUE, 8 avr. 2014, *Commission européenne* c. *Hongrie,* C-288/12, § 55.
[1781] V. art. 3 et 4 du règlement intérieur de la CNIL du 4 août 2020 qui encadrent strictement les incompatibilités.
[1782] V. art. 51 s. du règlement UE nº 2016/679. Pour une analyse, v. not. J. Deroulez, « Les autorités de contrôles en droit des données personnelles », *CCE* 2018, nº 4, dossier 7, § 10.
[1783] Art. 9 de la loi la loi nº 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018.

de la CNIL. Ce fut le cas en 2009, au sujet de la loi « Création et Internet »[1784]. Cette proximité avec le pouvoir politique est également marquée par la possibilité de renouvellement du mandat des membres. Une telle opportunité présente le risque de favoriser, particulièrement lors du premier mandat, une certaine discipline vis-à-vis de celui qui a le pouvoir de renouveler le mandat.

D'autre part, la présence d'un commissaire du gouvernement représentant ses intérêts auprès de la CNIL prouve le caractère relatif de l'indépendance de la Commission, au moins à l'égard du gouvernement. Cette présence témoigne d'une potentielle influence de l'exécutif, notamment parce que le commissaire du gouvernement assiste à toutes les délibérations de la formation plénière, aux réunions du bureau et aux séances de la formation restreinte (sans être pour autant présent au délibéré)[1785]. Le commissaire a également le pouvoir de provoquer une seconde délibération pour la plupart des décisions prises par la formation plénière[1786]. Ce rôle a été critiqué par la doctrine qui y voit une atteinte à l'indépendance de la Commission[1787]. Pour éviter une telle influence de l'exécutif, il serait parfaitement envisageable de restreindre la présence du commissaire du gouvernement aux seules affaires pour lesquelles celle-ci est nécessaire, c'est-à-dire lorsqu'il présente ses observations sur les projets de textes réglementaires. En effet, dans ces cas, sa présence est utile puisqu'il peut éclairer le collège sur le choix des mesures proposées.

En dehors de ces liens limités avec le pouvoir politique, le collège de la CNIL a une organisation structurelle favorisant son indépendance. De telles garanties ne se retrouvent pas dans les services de l'autorité.

B. Les faibles garanties d'indépendance des services de la CNIL

476. Les services de la CNIL. En avril 2014, les services de la CNIL ont largement été réorganisés. Cette réorganisation visait à s'adapter à l'environnement numérique et à placer les publics de l'institution au cœur de son activité[1788]. Les deux-cent-quinze

---

[1784] D. Forest, « Les limites intrinsèques de la garantie "d'indépendance" des autorités de contrôles. Le cas de la CNIL », *Dalloz IP/IT* 2016, p. 344.
[1785] Art. 17 al. 2 de la loi nº 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018.
[1786] Art. 17 de la loi nº 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018.
[1787] N. Poulet-Gibot Leclerc, *Droit administratif : sources, moyens, contrôles*, Bréal, 2007, p. 42 ; A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 2050, p. 710.
[1788] CNIL, *Rapport d'activité 2013,* La Documentation française, 2014, p. 8.

agents des services de la CNIL[1789], dirigés par le secrétaire général et le président, sont répartis en cinq directions : la direction de la conformité, chargée principalement de la mise en conformité des responsables de traitement ; la direction des relations avec les publics, chargée d'informer les différents publics, notamment les particuliers ; la direction de la protection des droits et des sanctions, chargée de s'assurer *a posteriori* de l'effectivité des droits des personnes ; la direction des technologies et de l'innovation, qui concentre une part de l'expertise technologique de la CNIL ; et la direction administrative et financière, regroupant les services supports de l'institution.

477. Une distinction excessive entre les services et le collège. La plupart des règles d'incompatibilité et d'indépendance prévues pour les membres du collège ne s'appliquent pas aux agents de la CNIL. Comme le remarquait Madame Marie-Anne Frison-Roche, « il est frappant que le dispositif légal soit à la fois très protecteur et très contraignant pour les membres du collège, mais n'existe pas de la même façon pour les membres des services techniques »[1790]. Cela tiendrait à l'idée selon laquelle seuls les membres du collège décident, tandis que les membres des services n'occuperaient qu'un rôle préparatif[1791]. Une telle conception est malmenée par la réalité du travail des services.

478. L'influence des services sur le travail du collège. Initialement considérés comme un appui aux besoins du collège, les services ont progressivement gagné en autonomie et en pouvoir. Un nombre conséquent d'agents travaillent en étroite collaboration avec le collège puisqu'ils préparent les dossiers, orientent le choix des contrôles[1792], les effectuent et en dressent les procès-verbaux[1793]. Il est peu contestable

---

[1789] En 1980, ils n'étaient que 28, v. CNIL, *Rapport d'activité 1978-1980,* La Documentation française, 1980, p. 22.

[1790] M.-A. Frison-Roche, « Étude dressant un bilan des autorités administratives indépendantes », in P. Gélard, « Rapport sur les autorités administratives indépendantes. Office parlementaire d'évaluation de la législation », Sénat, nº 404, 15 juin 2006, p. 75.

[1791] M.-A. Frison-Roche, « Étude dressant un bilan des autorités administratives indépendantes », in P. Gélard, « Rapport sur les autorités administratives indépendantes. Office parlementaire d'évaluation de la législation », Sénat, nº 404, 15 juin 2006, p. 75.

[1792] Les contrôles effectués par la CNIL ont des origines différentes : la majorité d'entre eux (62 %) sont effectués à l'initiative de la CNIL, notamment au vu de l'actualité. Les autres contrôles s'inscrivent dans le cadre de l'instruction de plaintes (17 %), du programme annuel décidé par les membres de la Commission (15 %) ou des suites de mises en demeure ou de procédures de sanction (6 %), v. CNIL, *Rapport d'activité 2017,* La Documentation française, 2018, p. 95.

[1793] En principe, le contrôle de la CNIL peut être effectué par un commissaire, le secrétaire général ou les agents habilités des services. En pratique, il est rare que les contrôles soient réalisés par d'autres personnes que les agents des services, v. A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nºs 2116 s., p. 710 s.

d'affirmer que celui qui prépare un dossier à une influence sur celui qui décide[1794]. Cette influence est d'autant plus probable que les membres qui décident ne sont pas des experts des technologies[1795] et n'exercent pas cette activité à temps plein[1796]. D'autres signes de la forte influence des services se retrouvent également dans les nombreux « guides pratiques » publiés, lesquels orientent la mise en conformité des organismes[1797]. Le travail des agents a donc une influence concrète et profonde sur l'activité de l'institution.

479. Le statut des agents. Les agents n'ont pas le statut de fonctionnaire et sont donc, pour la plupart, des agents contractuels de l'État. Un tel statut est relativement précaire puisque ces contrats durent en principe trois ans et ne sont renouvelables qu'une fois[1798]. Ainsi, les agents ne sont pas appelés à faire carrière au sein de l'autorité, et la question de la poursuite de celle-ci se pose.

Jusqu'en 2016, seules quelques situations marginales obligeaient les agents quittant leur fonction à saisir la commission de déontologie[1799]. Depuis 2016, tous les fonctionnaires et la plupart des agents non titulaires[1800] doivent informer leur administration de leur souhait d'exercer une activité dans une entreprise privée[1801]. En principe, l'administration est tenue de saisir la commission de déontologie de la

---

[1794] M.-A. Frison-Roche, « Étude dressant un bilan des autorités administratives indépendantes in P. Gélard, « Rapport sur les autorités administratives indépendantes. Office parlementaire d'évaluation de la législation », Sénat, nº 404, 15 juin 2006, p. 75.

[1795] V. *infra*, nº 489.

[1796] Seul le président de l'autorité exerce son activité à temps plein, v. art. 9 de la loi la loi nº 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018.

[1797] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 2037, p. 705.

[1798] Au-delà de ces six ans, les contractuels de l'État peuvent tenter d'être recrutés dans le cadre d'un contrat à durée indéterminée tel que le prévoit la loi nº 2012-347 du 12 mars 2012 relative à l'accès à l'emploi titulaire et à l'amélioration des conditions d'emploi des agents contractuels dans la fonction publique, à la lutte contre les discriminations et portant diverses dispositions relatives à la fonction publique, *JORF* 13 mars 2012, nº 0062, texte 4.

[1799] L'article 87 de la loi nº 93-122 du 29 janvier 1993 relative à la prévention de la corruption et à la transparence de la vie économique et des procédures publiques prévoyait une saisine obligatoire « pour les agents chargés soit d'assurer la surveillance ou le contrôle d'une entreprise privée, soit de conclure des contrats de toute nature avec une entreprise privée ou de formuler un avis sur de tels contrats, soit de proposer des décisions relatives à des opérations effectuées par une entreprise privée ou de formuler un avis sur de telles décisions », *JORF* 30 janv. 1993, nº 25, p. 1588.

[1800] En vertu du décret nº 2017-105 du 27 janvier 2017, sont concernés par cette obligation les agents non titulaires ayant été employés pendant six mois s'ils relèvent de la catégorie A ou un an pour les catégories B et C, v. article 1 du décret nº 2017-105 du 27 janvier 2017 relatif à l'exercice d'activités privées par des agents publics et certains agents contractuels de droit privé ayant cessé leurs fonctions, aux cumuls d'activités et à la commission de déontologie de la fonction publique, *JORF* 29 janv. 2017, nº 0025, texte 26.

[1801] La saisine de la commission de déontologie est obligatoire en toutes circonstances en cas de départ d'un agent vers le secteur privé, y compris pour les collaborateurs du président de la République, de cabinets ministériels ou d'élus locaux, v. A. Taillefait, « La mobilité entre le secteur public et le secteur privé : évolution ou agitation ? », *AJDA* 2018, p. 559. V. aussi, article 3 du décret nº 2017-105 du 27 janvier 2017 relatif à l'exercice d'activités privées par des agents publics et certains agents contractuels de droit privé ayant cessé leurs fonctions, aux cumuls d'activités et à la commission de déontologie de la fonction publique, *JORF* 29 janv. 2017, nº 0025, texte 26.

fonction publique, mais celle-ci peut aussi s'autosaisir dans les trois mois suivant l'embauche de l'agent.

480. L'attrait du secteur privé. Chaque année, de nombreux agents quittent les services de la CNIL pour mettre à profit les connaissances et relations acquises. La CNIL aurait ainsi un renouvellement annuel d'environ 10 % de ses agents[1802]. Pour chaque départ vers le secteur privé, la CNIL affirme saisir systématiquement la commission de déontologie. Cette dernière n'a pourtant jamais rendu d'avis d'incompatibilité[1803]. Néanmoins, les nombreux départs des agents vers des entreprises soumises aux contrôles de l'autorité engendrent des risques de pantouflage[1804]. Cette pratique désigne la situation de l'agent migrant vers le secteur privé où les relations acquises dans l'exercice de sa fonction publique pourront être sollicitées[1805]. Il est indéniable que lorsqu'un ancien agent de la CNIL devient responsable des affaires publiques, responsable en politique de confidentialité de Facebook ou encore responsable de la protection des données chez Criteo, il peut solliciter les relations acquises dans l'exercice de son ancienne fonction pour le bénéfice de son nouvel employeur[1806].

De manière surprenante, la CNIL valorise ces situations en considérant que cette mobilité contribue « à la bonne diffusion de la culture de la protection des données »[1807]. Pourtant de telles pratiques risquent d'engendrer des risques de partialité, voire des conflits d'intérêts, pour les agents des services[1808]. En effet, dès

---

[1802] E. Braün, « Données personnelles : les entreprises recrutent leurs experts dans l'administration », *Le Figaro* 1er janv. 2018.

[1803] Comme le remarque Monsieur Yves Mény, pendant longtemps en France il n'existait « ni réflexion ni règles de fond en la matière, mais seulement des procédures permissives et, exceptionnellement, des sanctions pour les cas jugés condamnables », Y. Mény, *La corruption de la République*, Fayard, 1992, p. 124. Ainsi, la Commission de déontologie n'a constaté des incompatibilités que dans 2 % de ses avis. La Commission explique ce faible chiffre en faisant valoir que cette « donnée ne saurait rendre compte, à elle seule, de la réalité et de la rigueur du contrôle de la commission. De nombreuses situations potentiellement risquées, y compris sur le plan pénal, sont désamorcées très en amont par l'administration en amenant à la renonciation aux fonctions privées envisagées ou par le rapporteur du dossier lors des entretiens avec l'agent concerné lorsque le dossier est parvenu jusqu'à l'instruction », F. Matras et O. Marleix, « Rapport d'information sur la déontologie des fonctionnaires et l'encadrement des conflits d'intérêts », Assemblée nationale, no 611, du 31 janv. 2018, p. 19.

[1804] Les conditions du délit de pantouflage, prévu par l'article 432-13 du code pénal, sont finalement assez restrictives et un faible nombre de situations entrent donc dans ce délit, v. *Rép. resp.* Dalloz, *Vo* « Responsabilité pénale des personnes publiques : infractions intentionnelles », par S. Corioland, 2019, nos 336 s.

[1805] A. Taillefait, « La mobilité entre le secteur public et le secteur privé : évolution ou agitation ? », *AJDA* 2018, p. 559.

[1806] Ces exemples sont issus de situations réelles, v. L. Boudard et D. Geiselhart, *Les possédés. Comment la nouvelle oligarchie de la tech a pris le contrôle de nos vies,* Arkhé, 2019, p. 158.

[1807] E. Braün, « Données personnelles : les entreprises recrutent leurs experts dans l'administration », *Le Figaro* 1er janv. 2018.

[1808] Il serait sans doute même possible de parler de risques de conflit d'intérêts. Selon Monsieur Thibault Douville, le conflit d'intérêt est « la situation dans laquelle un agent doit, à l'occasion d'une opération déterminée, trancher entre l'intérêt qui lui est confié et un autre intérêt », T. Douville, *Les conflits d'intérêts en droit privé*, th. Caen,

lors qu'ils ont le pouvoir d'orienter les contrôles, d'y participer et d'en établir les rapports, ne risquent-ils pas d'être tentés d'être moins rigoureux à l'occasion des contrôles d'entreprises dans lesquelles ils souhaiteraient ensuite être recrutés ? Le risque d'une certaine complaisance à l'égard de potentiels futurs employeurs est donc caractérisé. Par ailleurs, la confiance vis-à-vis des dires d'anciens collègues pourrait également altérer l'impartialité des contrôles effectués et la manière dont ces contrôles se déroulent. En effet, puisque d'anciens agents de la CNIL, recrutés par des entreprises, peuvent répondre aux agents de la CNIL en poste qui effectuent les contrôles, des risques de partialité émergent. En effet, la confiance établie lors de l'ancienne relation professionnelle pourrait réduire la rigueur du contrôle. Tous ces éléments portent atteinte à l'image d'indépendance et d'impartialité de l'autorité et risquent, sur le long terme, de porter préjudice à l'activité de la Commission[1809]. En effet, la théorie des apparences impose à chaque responsable public de donner de lui-même une image de parfaite indépendance et de probité afin de combattre la méfiance naturelle du peuple[1810].

481. Le pantouflage, problème récurrent des autorités de contrôle. L'autorité de contrôle française n'est pas la seule à être confrontée à ces risques de pantouflage et de conflit d'intérêts. L'agence fédérale de la protection des consommateurs aux États-Unis, la FTC, est dans une situation encore plus préoccupante puisque les trois-quarts de ses commissaires sont en situation de conflits d'intérêts avec des entreprises du numérique et d'autres industries[1811]. De tels conflits d'intérêts sont également présents, dans une moindre mesure toutefois, dans les services de l'agence fédérale.

482. Proposition : édicter des règles rigoureuses d'incompatibilité dans les services. Ces difficultés et risques commandent l'édiction de règles d'incompatibilité. Ces règles pourraient être appliquées aux agents dont les risques de conflits d'intérêts

---

2013, Institut universitaire Varenne, nº 374, p. 437. Pour autant, d'autres auteurs considèrent que le conflit d'intérêt se définit « moins comme une situation où se rencontrent, en une même personne, des intérêts opposés, que par les conséquences que cette opposition pourrait avoir sur l'accomplissement des fonctions de cette personne », C.-L. Vier, « La notion de conflit d'intérêts », *AJDA* 2012, p. 869.

[1809] La notion de conflit d'intérêts est fortement liée à la théorie des apparences, J.-J. Hyest, A. Anziani, N. Borvo Cohen-Seat, P.-Y. Colombat, Y. Détraigne, M.-A. Escoffier et J.-P. Vial, « Rapport d'information par le groupe de travail sur les conflits d'intérêts », Sénat, nº 518, 12 mai 2011, p. 10.

[1810] J.-J. Hyest, A. Anziani, N. Borvo Cohen-Seat, P.-Y. Colombat, Y. Détraigne, M.-A. Escoffier et J.-P. Vial, « Rapport d'information par le groupe de travail sur les conflits d'intérêts », Sénat, nº 518, 12 mai 2011, p. 35 ; A. Fittie-Duval, « La théorie des apparences, nouveau paradigme de l'action publique ? », *AJDA* 2018, p. 440.

[1811] R. Claypool, « The FTC's big tech revolving door problem. After decades of revolving door spinning, most top FTC officials have helped big tech and other corporate interests fight the FTC », *PublicCitizen* 23 mai 2019.

sont les plus grands, c'est-à-dire aux agents effectuant des missions de vérification ainsi qu'à ceux chargés des plaintes[1812]. Néanmoins, une telle solution n'est pas totalement satisfaisante puisque la plupart des agents sont habilités à effectuer ces missions de vérification[1813]. Cette solution aurait ainsi l'inconvénient d'établir des règles contraignantes pour des agents dont les risques de pantouflage ou de conflit d'intérêts sont plus réduits. Une solution alternative pourrait sans doute consister à favoriser le recrutement de fonctionnaires au sein de la direction de la protection des droits et des sanctions, notamment les services chargés des plaintes et des contrôles. En effet, les fonctionnaires bénéficient d'une position plus stable et ont moins tendance à utiliser leur expérience dans l'administration comme un tremplin pour leur carrière, ne serait-ce que parce que ces dernières se déroulent dans l'administration. Les agents non titulaires de cette direction pourraient également être soumis à des règles plus strictes d'incompatibilité ou à des délais les empêchant de rejoindre certaines branches du secteur privé[1814]. Une meilleure indépendance au sein des services de l'autorité de contrôle serait ainsi instaurée, renforçant la confiance dans les contrôles opérés par l'institution.

§ II. Renforcer les garanties procédurales devant la CNIL

483. D'importants pouvoirs confiés aux autorités de protection. Au fil des années, les autorités nationales de contrôle, et particulièrement la CNIL, ont vu leurs missions et prérogatives augmenter. Le règlement européen a été construit de façon à ce qu'elles en soient les garantes[1815]. Son article 57 prévoit, par exemple, que l'autorité contrôle l'application de ce texte et veille à son respect. Ces pouvoirs, et notamment sa capacité d'infliger des amendes administratives aux montants astronomiques, ont largement participé à la prise de conscience généralisée de l'importance du respect du droit des données à caractère personnel. Pour conserver la dynamique positive développée chez les responsables du traitement depuis l'entrée en vigueur du règlement européen, les autorités de contrôle doivent exercer pleinement leurs pouvoirs, et particulièrement

[1812] Sur l'importance de la prévention des situations d'incompatibilité pour réduire la probabilité des conflits d'intérêts, v. T. Douville, *Les conflits d'intérêts en droit privé*, th. Caen, 2013, Institut universitaire Varenne, nº 374, p. 437.
[1813] CNIL, délibération nº 2020-002 du 23 juillet 2020 habilitant des agents de la CNIL à procéder à des missions de vérification.
[1814] Y. Mény, *La corruption de la République*, Fayard, 1992, p. 136.
[1815] É. Gabrié, « Les pouvoirs des autorités de protection des données », *Dalloz IP/IT* 2017, p. 268.

celui d'imposer des amendes administratives[1816]. Dans le cas contraire, le droit des données à caractère personnel risque d'être un tigre de papier[1817].

484. La CNIL, une autorité aux fonctions juridictionnelles. À l'occasion des débats législatifs de 1977, les parlementaires avaient affirmé avec vigueur que la CNIL n'était pas une juridiction[1818]. C'est pour cette raison que l'autorité ne jouissait d'aucune prérogative juridictionnelle et que ses pouvoirs de contrôle et de sanction étaient quasi inexistants. En effet, entre 1978 et 2004, la réponse de la CNIL à un traitement de données personnelles ne respectant pas la loi se limitait à la prescription de mesures de sécurité, à un avertissement ou à une dénonciation au parquet[1819]. C'est dans cette logique que se sont inscrits les refus du Conseil d'État[1820] et du Conseil constitutionnel[1821] de qualifier, au regard du droit interne, les autorités administratives indépendantes comme des juridictions[1822]. Confronté à l'évolution des pouvoirs de ces autorités ainsi qu'à la jurisprudence de la CEDH, le Conseil d'État a dû assouplir cette position[1823] en reconnaissant que « les autorités administratives investies par la loi d'un pouvoir de sanction […] doivent, eu égard à leur nature, leur composition et leurs attributions être regardées comme des tribunaux au sens de l'article 6 § 1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales »[1824], et cela alors même qu'elles ne sont pas des juridictions au regard

---

[1816] C'est d'ailleurs « en matière de sanctions que se joue sans doute la crédibilité des pouvoirs des autorités », É. Gabrié, « Les pouvoirs des autorités de protection des données », *Dalloz IP/IT* 2017, p. 268.
[1817] C. Auffray, « Sanction Google : le RGPD n'est pas "un tigre de papier" », *ZDNet* 23 janv. 2019.
[1818] V. l'ensemble des débats à l'Assemblée nationale lors de la 2e séance du mardi 4 oct. 1977, *JORF AN* 5 oct. 1977, nº 79 (suite), p. 5803 s.
[1819] Art. 21 de la loi nº 78-753 du 17 juill. 1978.
[1820] CE Sec., 3 déc. 1999, *Caisse de crédit mutuel de Bain-Tresboeuf*, nº 197060 et nº 197061, *Lebon* p. 397.
[1821] À propos du Conseil de la concurrence, Cons. const., 23 janv. 1987, nº 86-224 DC, cons. 22 ; à propos du Conseil supérieur de l'audiovisuel, Cons. const., 17 janv. 1989, nº 88-248 DC, cons. 36 et Cons. const., 27 juill. 2000, nº 2000-433 DC, cons. 50 ; à propos de la Commission des Opérations de Bourse, Cons. const., 28 juill. 1989, nº 89-260 DC, cons. 18.
[1822] Une telle interprétation a été critiquée par la doctrine, v. not. S. Guinchard *et al.*, *Droit processuel. Droits fondamentaux du procès*, 10e éd., Dalloz, 2019, nº 334, p. 629 ; L. Boy, « Réflexions sur le "le droit de la régulation" », *D.* 2001, p. 3031, pour qui « la question du pouvoir juridictionnel ou quasi-juridictionnel des autorités administratives indépendantes n'interroge plus que quelques nostalgiques (…) de façon abstraite et théorique ». D'ailleurs, le Conseil d'État affirmait déjà dans son rapport de 2001 que « si le droit interne ne qualifie pas les autorités administratives indépendantes de juridictions, elles sont, quand elles engagent des procédures pouvant être suivies du prononcé d'une sanction – eu égard à leur nature, à leur composition et à leurs attributions – des tribunaux au sens de l'article 6 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH) », v. Conseil d'État, « Les autorités administratives indépendantes », *Rapport Public 2001*, La Documentation française, 2001, p. 360.
[1823] S. Guinchard *et al.*, *Droit processuel. Droits fondamentaux du procès*, 10e éd., Dalloz, 2019, nos 320 s, p. 577. Sur cette évolution et les divergences entre le Conseil d'État et la Cour de cassation sur cette qualification, v. J.-F. Brisson, « Les pouvoirs de sanction des autorités de régulation et l'article 6 § 1 de la Convention européenne des droits de l'homme à propos d'une divergence entre le Conseil d'État et la Cour de cassation », *AJDA* 1999, p. 847.
[1824] CE Sec., 10 mai 2004, *Crédit du Nord*, nº 241587, *Lebon T.* p. 693. Dans la décision de 2014 relative à la société Pages Jaunes, le Conseil d'État a considéré que lorsque la formation restreinte de la CNIL est saisie

du droit interne[1825]. Le Conseil d'État confirme donc que les autorités de contrôle doivent offrir toutes les garanties d'impartialité prévues par les stipulations de l'article 6 paragraphe premier de la CESDH.

485. Mise en place de garanties procédurales. L'exigence d'un procès équitable et public compte parmi les principes fondamentaux de toute société démocratique[1826]. Dès lors, avec le renforcement de l'arsenal de sanctions pouvant être prononcées par la CNIL, l'institution a progressivement mis en place de nouvelles garanties, notamment celles du procès équitable[1827]. Par exemple, depuis 2011, les fonctions de poursuite et de jugement sont séparées : les premières sont exercées par les membres de la CNIL n'appartenant pas à la formation restreinte alors que les secondes sont confiées aux membres de celle-ci[1828]. Une telle évolution était indispensable au regard du principe d'impartialité[1829], ce qui explique son accueil favorable par la doctrine[1830]. C'est surtout à l'égard des personnes concernées que la question des garanties procédurales est aujourd'hui la plus pressante.

486. Les réclamations. Le règlement européen place les autorités de contrôle au centre du dispositif de protection des personnes concernées. Celles-ci sont encouragées à présenter leurs réclamations à l'autorité. La réclamation est définie comme l'« acte par lequel un sujet de droit s'adresse à une autorité afin d'obtenir ce qu'il estime être son dû, de faire respecter son droit »[1831]. Ainsi, le choix de ce terme laisse penser que la personne ouvre, devant l'autorité, une action à l'encontre d'un responsable du

---

d'agissements pouvant donner lieu à l'exercice de son pouvoir de sanction ou d'avertissement, elle doit être regardée comme décidant du bien-fondé d'accusations en matière pénale, CE Sec., 12 mars 2014, *Société Pages Groupe,* n° 353193, *Lebon T.* p. 663. La Cour de cassation avait retenu une interprétation similaire en 1999 à l'égard de la Commission des Opérations de Bourse, Cass. Ass. plén., 5 févr. 1999, n° 97-16440, *Bull.* 1999, n° 1, p. 1. Dans une décision relative à l'Autorité de la concurrence, la Cour de cassation a affirmé que ces dispositions s'appliquent même en l'absence de dispositions spécifiques, Cass. civ. 2e, 4 juin 2020, n° 19-13.775, *NBP*. La CEDH a affirmé que la Commission bancaire française était un « tribunal » sur le fondement du paragraphe premier de l'article 6 de la CESDH et qu'elle décidait sur le « bien-fondé d'une accusation en matière pénale ». La CEDH s'attache donc à une appréciation *in concreto* des pouvoirs utilisés par les autorités, v. CEDH, 11 juin 2009, *Dubus S.A.* c. *France*, n° 5242/04, § 37.

[1825] CE Sec., 12 mars 2014, *Société Pages Groupe,* n° 353193, *Lebon T.* p. 663, § 3.

[1826] Sur les principes directeurs communs à toutes les procédures, v. S. Guinchard *et al.*, *Droit processuel. Droits fondamentaux du procès*, 10e éd., Dalloz, 2019, nos 748 s., p. 1315 s.

[1827] Sur les garanties procédurales devant les autorités administratives indépendantes, v. *Rép. pén.* Dalloz, *Vo* « Autorités administratives indépendantes », par A. Cappello, 2016 (actu. 2019), nos 117 s.

[1828] Loi n° 2011-334 du 29 mars 2011 relative au Défenseur des droits, *JORF* 30 mars 2011, n° 075, p. 5504, texte 2, reprise dans les art. 16 et 19 de la loi n° 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance n° 2018-1125 du 12 déc. 2018.

[1829] Sur la question du cumul des fonctions d'instruction et juridictionnel en matière de justice des mineurs, v. Cons. const., 8 juill. 2011, n° 2011-147 QPC, cons. 11.

[1830] H. Delzangles, « Un vent d'impartialité souffle encore sur le droit de la régulation », *AJDA* 2014, p. 1021.

[1831] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vo* « Réclamation ».

traitement ou d'un sous-traitant. Toutefois, la réclamation n'a pas un tel effet, puisqu'elle est traitée de manière discrétionnaire par l'autorité[1832]. À l'instar de la plainte simple ou de la dénonciation en droit pénal, la réclamation sert plutôt à *porter à la connaissance* de l'autorité certains faits qui sont considérés, par l'auteur de la réclamation, comme illicites[1833]. Son rôle est donc d'informer les autorités de contrôle compétentes des problèmes récurrents présents dans certains secteurs, tout en laissant aux autorités de contrôle une grande marge de manœuvre dans le traitement de cette information. Chaque année, la CNIL reçoit un nombre croissant de réclamations. De 4 821 réclamations déposées en 2010[1834], la CNIL en a reçu 14 137 en 2019[1835]. Pour traiter efficacement ces réclamations, les services de l'institution les organisent selon leur degré de complexité. Un traitement rapide est effectué pour les plaintes les moins complexes[1836], là où les plus complexes bénéficient d'une orientation vers le service des plaintes pour que soient opérés les actes d'instruction adéquats.

Dans le cas où l'autorité décide d'effectuer un contrôle ou de prendre une mesure particulière à l'encontre d'un organisme, le contentieux oppose uniquement l'autorité de contrôle à cet organisme. L'auteur de la réclamation initiale est considéré comme un tiers à la procédure et n'est donc jamais invité à présenter des observations. Pourtant, les réclamations proviennent parfois d'associations se faisant la voix de plusieurs centaines de personnes. C'est précisément la situation dans laquelle les associations La Quadrature du Net et *None of Your Business* se sont retrouvées lors de leurs réclamations collectives contre Google, formulées devant la CNIL en 2018[1837]. Si la CNIL a décidé d'instruire et de contrôler la conformité d'Android, le système d'exploitation de Google, les associations n'ont jamais été informées de l'évolution de

[1832] D'ailleurs il est fréquent de constater que la CNIL ouvre ses enquêtes uniquement lorsqu'une pluralité de personnes concernées ont effectué une réclamation contre un même organisme.
[1833] La dénonciation est « l'acte par lequel un tiers, qui n'a pas été lui-même victime de l'infraction, la porte à la connaissance des autorités de police ou de justice ; elle s'oppose alors à la "plainte", qui est une dénonciation émanant de la victime elle-même », B. Bouloc, *Procédure pénale,* 27e éd., Dalloz, 2019, no 486, p. 438. En vertu de l'article 40-1 du code de procédure pénale, le procureur décide de l'opportunité des poursuites, v. B. Bouloc, *Procédure pénale,* 27e éd., Dalloz, 2019, no 753, p. 661.
[1834] CNIL, *Rapport d'activité 2010,* La Documentation française, 2011, p. 13.
[1835] CNIL, *Rapport d'activité 2019,* La Documentation française, 2020, p. 2.
[1836] CNIL, *Rapport d'activité 2018*, La Documentation française, 2019, p. 42.
[1837] Le Conseil d'État a longtemps retenu une interprétation stricte de l'obligation d'information de la CNIL en considérant que « en s'abstenant d'informer M. X des suites réservées à son courrier, la commission n'a, en tout état de cause, pas méconnu les dispositions de l'article 54 de son règlement intérieur qui sont relatives à l'information des personnes dont la plainte fait l'objet d'une instruction par la commission », v. par ex. CE Sec., 6 févr. 2004, no 234016, inédit *Lebon*. Pour autant, une telle interprétation serait aujourd'hui contraire à la lettre du second paragraphe de l'article 77 du règlement européen.

la procédure, et cela en apparente violation de l'article 77 du règlement européen[1838]. Sur proposition du rapporteur, la formation restreinte de la CNIL avait conclu à la violation de plusieurs principes essentiels du droit des données à caractère personnel et prononcé une sanction exceptionnelle d'un montant de 50 millions d'euros[1839]. Les deux associations n'ont eu connaissance des suites données à leur plainte qu'au jour de la publication de cette délibération. Cette attitude non seulement pose un problème juridique, puisqu'elle est contraire aux règles prévues par le règlement européen, mais elle est aussi le reflet d'un problème symbolique de sous-valorisation du rôle des associations dans la mise en œuvre de ces règles[1840].

Il est donc impératif de renforcer les garanties procédurales à l'égard des auteurs de réclamation[1841]. La CNIL pourrait instaurer un système de suivi de l'état d'avancement des plaintes. En pratique, une page dédiée à la réclamation sur le site de la CNIL, offrant la possibilité de suivre les différents stades d'avancement du dossier suffirait[1842] : du dépôt de la plainte à la décision de la CNIL[1843]. Un tel système informerait l'auteur de la réclamation de son évolution, tout en l'autorisant à présenter des observations durant les différentes phases[1844]. D'ailleurs, il est possible de supposer que les auteurs de plaintes, particulièrement lors de plaintes collectives, ont acquis un savoir important sur les pratiques du responsable du traitement ou du sous-traitant, et que leurs observations sont susceptibles d'être pertinentes et d'aider les services d'enquête. Ainsi, et chaque fois qu'une procédure contentieuse est engagée, les auteurs de réclamations devraient être notifiés des différentes étapes de la procédure. Cette

---

[1838] Celui-ci impose pourtant, dans son deuxième paragraphe, que « l'autorité de contrôle auprès de laquelle la réclamation a été introduite informe l'auteur de la réclamation de l'état d'avancement et de l'issue de la réclamation ».

[1839] CNIL, délibération nº 2019-001 du 21 janvier 2019 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google LLC, spéc. nº 156. Cette délibération a été confirmée par le Conseil d'État, CE Sec., 19 juin 2020, *Société Google LLC*, nº 430810, *Lebon*.

[1840] L'autorité irlandaise fait l'objet de critiques similaires, v. not. NOYB, « Lettre ouverte sur les pourparlers "confidentiels" dans l'affaire Facebook », 24 mai 2020. Sur le besoin de renforcer le rôle des associations, v. *infra*, nº 536.

[1841] Dans son rapport sur l'application du règlement européen, la Commission européenne souhaitait également voir des avancées notamment, au niveau de « la participation des plaignants au cours de la procédure », Commission, COM2020 264, « Communication de la Commission au Parlement européen et au Conseil. La protection des données : un pilier de l'autonomisation des citoyens et de l'approche de l'Union à l'égard de la transition numérique – deux années d'application du règlement général sur la protection des données », 24 juin 2020, p. 6.

[1842] D'ailleurs, la désignation d'un rapporteur par le président de la CNIL constitue l'étape décisive de la procédure qui concrétise l'engagement des poursuites, v. A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 2170, p. 756.

[1843] Ces différentes étapes sont : réception, orientation aux services responsables, ouverture de l'enquête, actes d'instruction, notification du rapport, audience et décision.

[1844] Ces difficultés d'information se retrouvent également en droit pénal, particulièrement au sujet de la place de la victime dans le procès, v. *Rép. pén.* Dalloz, *Vº* « Action civile », par C. Ambroise-Castérot, 2017 (actu. 2020), nºs 16 s.

information non seulement est fondée sur une bonne administration de la justice, mais garantit surtout une forme de contradictoire[1845]. D'ailleurs, le règlement intérieur de la CNIL offre la possibilité à un tiers d'intervenir dans une affaire « dès lors que celui-ci détient un intérêt manifeste dans l'affaire et que cette intervention se rattache indiscutablement à l'objet de la procédure »[1846]. Dès lors, il semble logique de permettre aux auteurs de réclamations, à l'instar des tiers ayant un intérêt dans l'affaire, de présenter des observations. Pour ce faire, les auteurs des réclamations devraient être mieux informés de l'avancée de la procédure devant l'autorité de contrôle.

487. La publicité des activités de la formation restreinte. En général, le principe de publicité des débats vise à « protéger les justiciables contre une justice secrète échappant au contrôle du public »[1847] et s'inscrit donc logiquement dans la démocratie participative actuelle. La publicité des débats est reconnue comme un principe constitutionnel par le Conseil constitutionnel[1848] tout en étant consacrée dans les grandes déclarations internationales de droits[1849]. En outre, le Conseil d'État l'analyse comme un principe général du droit[1850]. Cette publicité est textuellement garantie par l'article L. 6 du code de justice administrative pour l'ordre administratif[1851], et par l'article 22 du code de procédure civile ainsi que par les articles 306 et 400 du code de procédure pénale pour l'ordre judiciaire. Ceci justifie donc le caractère public des séances de la formation restreinte de la CNIL[1852]. Pour autant, n'est que récemment que

---

[1845] Cette critique est parfaitement transposable à d'autres autorités indépendantes, particulièrement à la Commission d'accès aux documents administratifs, devant laquelle l'administré est dans un conflit l'opposant directement à l'administration. Pourtant, l'administré n'a jamais la possibilité de présenter ses observations.
[1846] Article 63 du règlement intérieur de la CNIL du 4 août 2020.
[1847] CEDH, 23 juin 1981, *Le Compte, Van Leuven et de Meyere* c. *Belgique*, n° 6878/75 et n° 7238/75, § 59 ; CEDH, 12 juill. 2001, *Malhous* c. *République Tchèque*, n° 33071/96, § 55.
[1848] Le Conseil constitutionnel déduit le principe de publicité du procès pénal des articles 6, 8, 9 et 16 de la Déclaration des droits de l'homme et du citoyen, v. Cons. const., 2 mars 2004, n° 2004-492 DC, cons. 117. Depuis la décision du 21 mars 2019, le Conseil constitutionnel reconnaît un principe constitutionnel de publicité des audiences devant les juridictions civiles et administratives. Ce principe est fondé sur les articles 6 et 16 de la Déclaration des droits de l'homme et du citoyen, Cons. const., 21 mars 2019, n° 2019-778 DC, cons. 102.
[1849] L'article 14 du Pacte international relatif aux droits civils et politiques, l'article 6 paragraphe 1 er de la CESDH et l'article 47 de la Charte des droits fondamentaux de l'Union européenne.
[1850] CE Ass., 4 oct. 1974, *Dame David*, n° 88930, *Lebon* p. 464.
[1851] Depuis l'ordonnance du 2 février 1831, l'audience n'est plus secrète devant le Conseil d'État. Cette ordonnance a institué les débats publics devant cette juridiction, v. *Rép. cont. adm.* Dalloz, *V°* « Jugement », par V. Haïm, 2017 (actu. 2020), n^os^ 60 s.
[1852] L'article 65 alinéa 2 du règlement intérieur de la CNIL du 4 août 2020 prévoit en effet que « le président de séance peut, à la demande du responsable de traitement mis en cause ou à son initiative, restreindre la publicité de l'audience dans l'intérêt de l'ordre public, ou lorsque la protection de secrets protégés par la loi l'exige ». C'était d'ailleurs le souhait de certains sénateurs du groupe socialiste qui avaient proposé en 1977 d'insérer un article additionnel ouvrant la possibilité au public d'assister « directement ou par retransmission simultanée à toute réunion de la commission » et mettant à la disposition du public « les comptes rendus des débats ouverts au public ainsi que les annonces relatives aux réunions à venir », v. amendement n° 105, séance du 17 nov. 1977, *JORF S* 18 nov. 1977, n° 77, p. 2787.

cette publicité est devenue effective grâce à la publication, sur le site de la CNIL, des dates de réunion de cette formation[1853]. Dans l'objectif de plus grande transparence des travaux de la formation, il serait envisageable d'ajouter, en plus de la date de la séance, l'ordre du jour de celle-ci afin de mieux informer le public[1854].

488. La publicité des sanctions. Parmi les garanties prévues à l'article 6 paragraphe premier de la CESDH figure assurément le principe de publicité de la décision qui, pour la CEDH, ne trouve que des exceptions strictement encadrées[1855]. Comme le remarque une opinion doctrinale, « il est important en effet que les tiers puissent accéder au jugement, comme ils ont accès aux audiences ; c'est l'un des buts de la règle de publicité de la justice, que de permettre "le contrôle du public" »[1856]. Cette publicité vise à protéger les justiciables contre une justice secrète et constitue ainsi l'un des moyens de préserver la confiance du public dans les cours et les tribunaux[1857]. Dès lors que l'on reconnaît aux autorités administratives, et particulièrement à la CNIL, la qualité de tribunal au sens de l'article 6 paragraphe 1er de la CESDH[1858], l'intégralité des garanties de cet article, notamment celle de publicité des décisions, doivent leur être appliquées[1859].

Selon l'étude d'impact du 12 décembre 2017 du projet de loi relatif à la protection des données personnelles, et conformément à la jurisprudence du Conseil d'État, la décision de rendre publique une sanction prononcée par la CNIL aurait le caractère d'une sanction complémentaire[1860]. Le législateur français a donc établi un principe d'opacité des décisions prononcées par la CNIL, avec une publicité optionnelle et décidée au cas par cas. En effet, l'article 20 de la loi Informatique et

---

[1853] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 2206, p. 770. Il s'agissait précisément d'une demande formulée à l'institution puis, à défaut de réponse de celle-ci, à la CADA par l'auteur de ces lignes, laquelle a abouti rapidement.
[1854] C'est actuellement le cas pour l'ordre du jour des séances de la formation plénière du collège de la CNIL.
[1855] CEDH, 28 juin 1984, *Campbell et Fell* c. *Royaume-Uni*, nº 7819/77 et nº 7878/77, § 90. Monsieur Nicolas Braconnay rappelle que « la publicité du prononcé de la décision ne souffre (…) aucune exception, qu'il soit fait par lecture à l'audience ou par dépôt au greffe. Dans tous les cas, les tiers peuvent se faire délivrer gratuitement une copie de la décision. La loi du 23 mars 2019 prévoit en outre la mise "à la disposition du public à titre gratuit sous forme électronique" de l'ensemble des décisions de justice, dans le respect de la vie privée des parties et des tiers », N. Braconnay, *La justice et les institutions juridictionnelles*, 3e éd., La Documentation française, 2019, p. 21.
[1856] S. Guinchard *et al.*, *Droit processuel. Droits fondamentaux du procès*, 10e éd., Dalloz, 2019, nº 596, p. 1051.
[1857] CEDH, 22 févr. 1984, *Sutter* c. *Suisse*, nº 8209/78, § 26.
[1858] V. *supra*, nº 484.
[1859] *Rép. pén.* Dalloz, *Vº* « Autorités administratives indépendantes », par A. Cappello, 2016 (actu. 2019), nº 207.
[1860] CE Sec., 27 juill. 2012, *Société AIS 2,* nº 340026, *Lebon T.* p. 766, § 6. Selon l'étude d'impact du projet de loi relatif à la protection des données personnelles, la publicité de la sanction « n'est pas prévue par le règlement », v. Gouvernement, « Étude d'impact Projet de loi relatif à la protection des données personnelles », 12 déc. 2017, p. 60.

libertés laisse au président de la CNIL la discrétion de rendre publiques les mises en demeure prononcées par le bureau, et son article 22 offre ce même choix à la formation restreinte pour les mesures qu'elle adopte. Pourtant, le règlement européen ne distinguant pas entre la publicité ou l'opacité des mesures coercitives[1861], l'adage *ubi lex non distinguit, nec nos distinguere debemu* doit s'appliquer[1862]. D'ailleurs, le considérant 129 de ce texte rappelle que « les pouvoirs des autorités de contrôle devraient être exercés conformément aux garanties procédurales appropriées prévues par le droit de l'Union et le droit des État membres ». Une telle affirmation implique nécessairement le respect du principe de publicité des décisions. Comme le souligne une opinion doctrinale, la publicité de la sanction constitue « une mesure plus redoutable – et redoutée – que le quantum ou la nature même de la sanction »[1863]. Le droit français doit donc évoluer pour garantir la publicité de *l'ensemble des décisions* prononcées par la CNIL.

§ III. Renforcer la mixité de profils au sein de la CNIL

489. Des profils principalement juridiques. Parmi les deux-cent-quinze agents de l'institution, cent-trente sont habilités à effectuer des missions de vérification[1864]. Seuls vingt d'entre eux – soit 15 % – occupent des postes techniques[1865]. Ce faible chiffre contraste fortement avec les soixante-deux juristes habilités à effectuer ces missions de vérification. Pourtant, ces missions nécessitent d'importantes compétences techniques et une bonne compréhension des systèmes d'information, notamment pour vérifier la conformité des pratiques de l'organisme à sa documentation et au droit. Par exemple, lorsque la CNIL effectue un contrôle, ses agents doivent être capables de déterminer la validité des arguments invoqués par l'organisme. Par exemple, s'il justifie son traitement sur le fondement des intérêts légitimes, notamment pour des raisons de

[1861] L'ensemble des mesures coercitives prévues par le paragraphe 2 de l'article 58 du règlement UE nº 2016/679 ne mentionnent pas de mesure de publicité parmi l'éventail de sanctions qu'il prévoit.
[1862] Sur la publicité des jugements, v. CEDH, 8 déc. 1983, *Pretto* c. *Italie*, nº 7984/77, § 25 s.
[1863] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 2206, p. 770. Ce qui rappelle le principe du *name and shame* du droit de la *compliance*, lequel irrigue toutes les branches du droit, v. N. Cuzacq, « Le mécanisme du *name and shame* ou la sanction médiatique comme mode de régulation des entreprises », *RTD com.* 2017, p. 473.
[1864] Les missions de vérification sont les missions pendant lesquelles les agents peuvent avoir accès, de 6 heures à 21 heures, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel, v. art. 19 de la loi nº 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018.
[1865] CNIL, délibération nº 2020-002 du 23 juillet 2020 habilitant des agents de la CNIL à procéder à des missions de vérification.

sécurité, les agents devraient pouvoir évaluer cet argument en comparant avec les alternatives techniques moins invasives qui réaliseraient le même objectif[1866].

Ces compétences techniques et technologiques sont encore moins bien représentées au sein du collège de la CNIL. En effet, les connaissances des commissaires sont surtout centrées autour du droit, des sciences sociales ou de la politique, et très peu d'entre eux ont une formation technique ou des compétences particulières en informatique[1867]. Cette faible représentation de profils techniques est particulièrement problématique dès que ces commissaires sont invités à se positionner sur les technologies utilisées et à l'occasion des contrôles. En 1998, Guy Braibant déplorait déjà que « les représentants des pouvoirs publics, des juridictions et de l'administration, bref du secteur public, y ont une place prépondérante, et la société civile une place trop réduite, qui ne se justifie plus aujourd'hui. Dans le même ordre d'idées, les juristes sont en situation de quasi-monopole, et les informaticiens absents »[1868].

Ces observations amènent deux types de commentaires. D'une part, la CNIL doit se doter, en interne, d'une meilleure mixité de profils, pour créer des synergies et de la transdisciplinarité, essentielle dans une institution dont la mission principale est de comprendre et réguler les implications de l'informatique sur les libertés[1869]. D'autre part, la CNIL ne peut être la seule à promouvoir le respect du droit des données personnelles, et d'autres types de contrôle doivent donc être valorisés.

SECTION II – LES AUTRES CONTRÔLES

490. Limites à l'action de la CNIL. Depuis son apparition en 1978, la CNIL n'a cessé de dénoncer l'inadéquation de ses moyens par rapport à l'étendue de ses missions. Ce déséquilibre s'est renforcé à l'occasion des extensions successives de ses pouvoirs. Puisque le nombre d'infractions aux règles du droit des données personnelles excède largement les capacités de contrôle des autorités, il est évident que ces dernières ne

[1866] Sur la question de la validité de l'intérêt légitime pour fonder un traitement de données (collecte de cookies) pour des non-utilisateurs de Facebook, la saga judiciaire opposant Facebook à la Commission de la protection de la vie privée belge offre un éclairage intéressant, v. not. A. Michel, « Le traçage comportemental des internautes sur les réseaux sociaux : l'affaire des "cookies Facebook", véritable saga judiciaire ? », *Revue du droit des technologies de l'information* 2019, nº 74, p. 72, spéc. p. 88 s.
[1867] Sur les profils des présidents de la CNIL, v. *infra*, nº 530.
[1868] G. Braibant, « Données personnelles et société de l'information. Rapport au Premier ministre sur la transposition en droit français de la directive nº 95/46 », La Documentation française, 1998, p. 87.
[1869] Plus généralement, N. Martial-Braz, « La transdisciplinarité du droit du numérique », in *Mélanges M. Vivant*, 2020, Dalloz, p. 849 s., nº 16, spéc. p. 860.

peuvent être les seules à garantir le respect du droit des données personnelles[1870]. Comment assurer une meilleure diffusion de la culture de protection des données personnelles au sein même des organismes traitant des données à caractère personnel ? La question est capitale, notamment parce que la nouvelle notion appelle une meilleure compréhension des enjeux de protection des personnes et une plus grande responsabilité des organismes.

491. Plan. L'heure actuelle n'est pas à l'augmentation considérable de la dépense publique[1871] et l'autorité de contrôle doit donc emprunter des chemins audacieux pour amplifier son action. Pour cela, elle doit pouvoir s'appuyer sur des contrôles internes (§ I) et développer de nouvelles collaborations (§ II).

§ I. Le renforcement des contrôles internes à l'organisme

492. Plan. Au sein des organismes, deux types de profil favorisent une meilleure mise en œuvre de la protection des personnes. Il s'agit du délégué à la protection des données (A) et des experts techniques (B).

A. Le délégué à la protection des données

493. La logique de responsabilisation. Les mécanismes d'autorégulation dans le droit des données personnelles préexistaient au règlement européen[1872]. En effet, la directive 95/46 reconnaissait déjà leur pertinence, en envisageant notamment la désignation d'un détaché à la protection des données comme un moyen pour les États membres de prévoir, dans leur droit, des dispenses de formalités[1873]. Le règlement

---

[1870] Comme le constataient déjà en 2003 Messieurs Beauvallet, Flichy et Ronai, « même en renforçant les pouvoirs d'investigation et de sanction des autorités de contrôle, même en augmentant leurs moyens humains, on pressent que le modèle européen fondé sur une autorité de contrôle atteint ses limites face à l'explosion des fichiers et des traitements, à la flexibilité des outils informatiques, à la vitesse de leur évolution, à la complexité des architectures mises en place », G. Beauvallet, P. Flichy et M. Ronai, « Incorporer la protection de la vie privée dans les systèmes d'information, une alternative à la régulation par la loi ou par le marché », *Terminal* 2003, nº 88, p. 89.

[1871] Il est toutefois remarquable que le projet de loi de finances pour 2021 accorde à la CNIL 20 emplois supplémentaires, Ministère de l'économie des finances et de la relance, « Projet de Loi de Finances 2021. La relance », 28 sept. 2020, p. 93.

[1872] Pour une analyse du rôle de la CNIL dans cette évolution, v. C. Koumpli, *Les données personnelles sensibles. Contribution à l'évolution du droit fondamental à la protection des données à caractère personnel*, th. Paris I, 2019. Pour plus de détails, v. *supra*, nº 309.

[1873] Art. 18 § 2 de la directive CE nº 95/46. Le choix du terme « détaché » illustrait bien la proximité de cette fonction avec le rôle de la CNIL. D'ailleurs, le rapport Braibant n'hésitait pas à considérer que « ce délégué serait investi d'une véritable mission de contrôle, qu'il exercerait en lieu et place de la CNIL puisqu'il serait chargé de veiller à l'application de la loi, de procéder à l'examen préalable des traitements qui y sont soumis, et d'assurer la publicité des traitements, v. G. Braibant, « Données personnelles et société de l'information. Rapport au Premier ministre sur la transposition en droit français de la directive nº 95/46 », La Documentation française, 1998, p. 73.

européen n'a fait qu'amplifier ce mouvement. Ainsi, la protection des données n'est plus centrée autour de l'action de la CNIL, mais s'opère au cœur même des organismes traitant des données personnelles[1874]. Au sein de ces organismes, le chef d'orchestre de la conformité est souvent incarné par le délégué à la protection des personnes.

494. Le Correspondant Informatique et Libertés. La transposition de la directive 95/46 a été l'occasion d'introduire en droit français la fonction Correspondant Informatique et Libertés. Cette proposition avait été accueillie avec d'importantes réserves, tant par le rapport Braibant[1875] qu'à l'occasion des débats parlementaires[1876]. En dépit de cette frilosité, le législateur a finalement instauré cette fonction[1877], dont les principes ont été validés par le Conseil constitutionnel[1878]. De l'avis de la CNIL, ce correspondant apporte une aide précieuse à l'organisme en ayant un rôle de conseil et de suivi dans la légalité du déploiement des projets informatiques et, plus largement, de la gestion des données à caractère personnel[1879]. Dès 2006, Madame Nathalie Métallinos n'hésitait pas à considérer le Correspondant Informatique et Libertés comme le « garant de l'effectivité de la loi »[1880]. Au fil des ans, en France comme ailleurs, cette fonction n'a cessé de prendre de l'importance, et la consécration par le règlement européen de la fonction de délégué à la protection des données s'est donc faite naturellement[1881].

495. Le délégué à la protection des données. Conformément à la logique actuelle du droit des données à caractère personnel, les organismes qui traitent ces données doivent mettre en place les mesures techniques et organisationnelles appropriées pour

---

[1874] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 2239, p. 782.
[1875] G. Braibant, « Données personnelles et société de l'information. Rapport au Premier ministre sur la transposition en droit français de la directive nº 95/46 », La Documentation française, 1998, p. 72 s.
[1876] A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, nº 2237, p. 782.
[1877] C'est le Sénat qui a introduit dans la loi Informatique et libertés la possibilité pour les organismes de désigner un tel correspondant, v. R. de Quenaudon, « La cote mal taillée du salarié correspondant à la protection des données à caractère personnel », *Revue droit du travail* 2006, p. 32.
[1878] Cons. const., 29 juill. 2004, nº 2004-499 DC, cons. 21 s.
[1879] G. Vercken, G. Van Ossel et C. Serpagli, « Le "correspondant à la protection des données" : une création inachevée ? », *RLDI* 2005, nº 9, p. 58.
[1880] N. Métallinos, « Maîtriser le risque Informatique et Libertés. La mise en place du correspondant à la protection des données personnelles », *Droit Social* 2006, p. 378.
[1881] G. Péronne et E. Daoud, « L'évolution du rôle du CIL à la lumière du nouveau règlement européen sur les données personnelles », *Dalloz IP/IT* 2016, p. 192. Sur la différence entre le délégué à la protection des données et le Correspondant Informatique et Libertés, O. Tambou, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, nº 312, p. 281.

s'assurer de leur conformité et être en mesure de la démontrer[1882]. La vigilance des organismes doit donc être continue, c'est-à-dire qu'elle ne se limite pas à une mise en conformité au moment de la création du traitement, mais résulte bien d'un processus dynamique et continu. Plus que jamais, le règlement européen dessine les contours d'une culture juridique fondée sur l'autorégulation, dont le délégué à la protection des données est la cheville ouvrière[1883]. Par principe, la désignation du délégué à la protection des données est facultative, puisque le règlement européen reconnaît seulement trois cas de désignation obligatoire[1884]. En pratique, ces trois cas couvrent un très grand nombre de situations, et même lorsque cette désignation n'est pas obligatoire, elle est souvent accomplie parce qu'elle est considérée comme une bonne pratique d'entreprise, illustrant une gestion proactive de la protection des données personnelles[1885].

Le délégué à la protection des données assure plusieurs fonctions et ce, tout au long du cycle opérationnel de vie des traitements[1886]. En tant que pilote de la conformité, il doit être associé à toutes les questions relatives à la protection des données[1887]. Dans le cadre de cette fonction, il informe et conseille le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement[1888]. En outre, ses missions incluent l'organisation de la documentation et l'identification des processus au sein de l'organisme garantissant le respect des principes de protection des données[1889]. En tant qu'auditeur, le délégué est tenu de contrôler, au sein de l'organisme, le respect du règlement européen[1890] en analysant et vérifiant la

---

[1882] Art. 5 § 2 et 24 du règlement UE nº 2016/679. Pour une étude de ces articles, v. not. C. de Terwangne et K. Rosier, *Le règlement général sur la protection des données. Analyse approfondie,* Larcier, 2018, nºs 24 s.

[1883] G. Péronne et E. Daoud, « L'évolution du rôle du CIL à la lumière du nouveau règlement européen sur les données personnelles », *Dalloz IP/IT* 2016, p. 192.

[1884] Les trois cas de saisine concernent les situations dans lesquelles les traitements ont le plus grand risque d'avoir un impact sur les personnes puisqu'il s'agit des traitements effectués par une autorité publique ou un organisme public (sauf les juridictions), des traitements qui exigent un suivi régulier et systématique à grande échelle des personnes concernées et des traitements à grande échelle de données sensibles ou relatives à des condamnations pénales, v. *JCl. comm.,* fasc. 942, « Le délégué à la protection des données (DPD) », par G. Desgens-Pasanau, 2018, nº 6. Le G29 recommande que les responsables du traitement et les sous-traitants documentent l'analyse interne effectuée afin de démontrer que les facteurs pertinents ont été correctement pris en considération, G29, WP 243 rév. 01, Lignes directrices concernant les délégués à la protection des données (DPD), 5 avr. 2017, p. 7.

[1885] A. Carrera Mariscal, « Le CIL : modèle type du futur délégué à la protection des données ? », *Dalloz IP/IT* 2018, p. 233.

[1886] A. Carrera Mariscal, « Le CIL : modèle type du futur délégué à la protection des données ? », *Dalloz IP/IT* 2018, p. 233.

[1887] G29, WP 243 rév. 01, Lignes directrices concernant les délégués à la protection des données (DPD), 5 avr. 2017, p. 16.

[1888] Art. 39 § 1 c) du règlement UE nº 2016/679.

[1889] Cette documentation est mise en œuvre par la création des procédures, guides, documents de recensement et d'instruction des traitements, v. A. Carrera Mariscal, « Le CIL : modèle type du futur délégué à la protection des données ? », *Dalloz IP/IT* 2018, p. 233.

[1890] A. Carrera Mariscal, « Le CIL : modèle type du futur délégué à la protection des données ? », *Dalloz IP/IT* 2018, p. 233.

conformité des activités de traitement ainsi que, le cas échéant, en formulant des recommandations[1891]. Enfin, en tant que facilitateur, le délégué est également le point de contact de l'autorité de contrôle et des personnes concernées[1892].

Sa place est si centrale que ses rapports d'activités sont directement transmis au niveau le plus élevé de la direction de son organisme[1893]. Face à la diversité et à l'importance de ses missions, il était essentiel d'organiser son indépendance.

496. La place du délégué à la protection des données dans l'organisme. Le règlement européen octroie aux responsables du traitement une importante flexibilité dans le choix de leur délégué. Un groupe d'entreprises[1894] ou un groupe d'organismes du secteur public[1895] peut ainsi mutualiser son délégué[1896], c'est-à-dire n'en désigner qu'un pour des entités pourtant juridiquement distinctes. Par ailleurs, le délégué peut être interne (membre du personnel) ou externe (exercer ses missions sur la base d'un contrat de service) à l'organisation[1897]. Bien sûr, le délégué à la protection interne à l'organisme a une assise plus importante au sein de celui-ci puisqu'il est connu de tous et « connaît l'entreprise sur le bout des doigts : il est mieux à même de découvrir l'existence d'un projet impliquant des données personnelles au détour d'une conversation anodine devant la machine à café ou dans le compte-rendu d'une réunion »[1898]. Le choix d'un délégué externe implique de vérifier la compatibilité du statut du prestataire avec les fonctions du délégué[1899]. Pour autant, l'un des avantages du délégué externe est son extériorité et sa neutralité à l'égard de l'organisme, favorisant ainsi son indépendance.

497. L'indépendance du délégué à la protection des données. Le règlement européen prévoit plusieurs dispositions pour garantir l'indépendance du délégué à la

---

[1891] G29, WP 243 rév. 01, Lignes directrices concernant les délégués à la protection des données (DPD), 5 avr. 2017, p. 20.
[1892] Art. 39, § 1 d) et e) du règlement UE nº 2016/679.
[1893] Art. 38 § 3 du règlement UE nº 2016/679.
[1894] Art. 37 § 2 du règlement UE nº 2016/679.
[1895] Art. 37 § 3 du règlement UE nº 2016/679.
[1896] Sur le rôle et l'organisation des délégué à la protection des données au sein des grands organismes, v. J. Godin et E. Lemoalle, « Le rôle de *Data Protection Officer* à l'international, une étude comparative », *Dalloz IP/IT* 2018, p. 293.
[1897] *Rép. eur.* Dalloz, *Vº* « La protection des données personnelles dans les relations internes à l'Union européenne », par C. Castets-Renard, 2018 (actu. 2020), nº 136 ; O. Tambou, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, nº 314, p. 281.
[1898] B. Rasle, « RGPD : faut-il désigner un DPO interne ou un DPO externe », *Cyber-Risques* 15 janv. 2020.
[1899] La question s'est posée au sujet des avocats, *JCl. comm.,* fasc. 942, « Le délégué à la protection des données (DPD) », par G. Desgens-Pasanau, 2018, nº 12.

protection des données, laquelle se manifeste à plusieurs niveaux[1900]. Organique tout d'abord, puisque le délégué doit exercer ses missions avec un degré suffisant d'autonomie et sans recevoir d'instruction dans leur mise en œuvre. En principe, il ne peut donc pas être relevé de ses fonctions ou pénalisé pour leur exercice[1901]. Un régime de prévention des conflits d'intérêts lui est également imposé pour les autres missions dont il peut être chargé. Cette indépendance est également fonctionnelle puisque le délégué doit bénéficier des ressources nécessaires pour l'exercice de ses missions[1902]. Ces ressources doivent être en adéquation avec les opérations de traitement, et le délégué doit avoir suffisamment de temps, de soutien dans ses fonctions et de ressources matérielles et économiques[1903]. Le délégué à la protection des données est donc l'une des « pierres angulaires du régime de responsabilité »[1904]. En pratique, la mise en œuvre concrète de ce rôle de vigie reste parfois semée d'embuches.

498. Les limites à la fonction de délégué comme organe de contrôle interne. Plusieurs limites entravent l'effectivité de l'action du délégué à la protection des données. Tout d'abord, le règlement européen ne prévoit rien en cas de désaccord entre le délégué et le responsable du traitement ou le sous-traitant. En effet, le texte dispose qu'il est « associé (…) à toutes les questions relatives à la protection des données à caractère personnel ». Mais le texte est avare en détail quant aux modalités de résolution d'un désaccord sur cette mise en conformité. Dans ce type de situation, le délégué à la protection des données demeure relativement isolé puisqu'il n'existe pas d'organe central de conseil[1905]. Le délégué pourra quand même contacter la CNIL sans en informer son organisation, mais une telle action pourrait être perçue comme déloyale par celle-ci[1906].

Par ailleurs, en ce qui concerne le profil du délégué à la protection des données, le règlement européen prévoit que celui-ci doit avoir des « connaissances spécialisées

---

[1900] Art. 38 du règlement UE nº 2016/679.
[1901] Art. 38 § 3 du règlement UE nº 2016/679. Le G29 précise toutefois que « le RGPD n'interdit les sanctions que si elles sont imposées au DPD à la suite de l'exercice de ses missions de DPD », G29, WP 243 rév. 01, Lignes directrices concernant les délégués à la protection des données (DPD), 5 avr. 2017, p. 18.
[1902] Art. 38 § 2 du règlement UE nº 2016/679.
[1903] G29, WP 243 rév. 01, Lignes directrices concernant les délégués à la protection des données (DPD) », 5 avr. 2017, p. 17.
[1904] G29, WP 243 rév. 01, Lignes directrices concernant les délégués à la protection des données (DPD), 5 avr. 2017, p. 5.
[1905] Il existe tout de même certaines associations qui regroupent ces délégués à la protection des données, v. par ex. l'AFCP (l'Association Française des Correspondants à la Protection des données à caractère personnel).
[1906] E. Scaramozzino, « *Open data* versus protection des données : les enjeux pour le tourisme des *smart cities* », *Juris tourisme* 2018, nº 207, p. 24.

du droit et des pratiques en matière de protection des données »[1907]. Selon le G29, il est nécessaire que les délégués disposent d'une expertise dans le domaine des législations et pratiques nationales et européennes en matière de protection des données, ainsi que d'une connaissance approfondie du droit des données personnelles[1908]. Ainsi, c'est la maîtrise du droit qui l'emporte sur les connaissances techniques puisque le règlement et le G29 ne s'y réfèrent que pour désigner une qualité supplémentaire. Une telle approche de la conformité est regrettable puisque les connaissances juridiques semblent préférées aux connaissances technologiques. En effet, dès lors que le délégué n'est pas un expert des technologies, ses analyses risquent de rester principalement juridiques. Le délégué ne sera sans doute pas en capacité de proposer des alternatives technologiques plus respectueuses de la vie privée[1909]. En pratique, cela limite sa capacité à comprendre l'ensemble des implications de la technologie sur laquelle il est consulté. Dès lors, il sera dépendant des dires des employés et risque d'être enfermé dans un modèle technologique, sans pouvoir être force de propositions alternatives. Fort heureusement, la réalité montre un paysage plus nuancé, et les profils issus de la conformité ou de l'informatique sont représentés en nombre parmi les délégués à la protection des données[1910].

Enfin, si le statut de délégué à la protection des données est trop récent pour mesurer son impact sur le respect du droit des données personnelles, une enquête effectuée en 2015 sur les Correspondants Informatique et Libertés dressait déjà quelques constats. La majorité des correspondants exerçaient leur fonction moins de deux jours par mois et la moitié d'entre eux n'avaient mis aucune procédure en place pour traiter les réclamations ou pour organiser les équipes en cas de contrôle de la CNIL[1911]. Plus surprenant encore, aucune des organisations pour lesquelles ces correspondants travaillaient n'avait été soumise à un contrôle de la CNIL[1912]. Bien que la plupart de ces constats aient été confirmés par une étude menée en 2020, la fonction

---

[1907] Art. 37 § 5 du règlement UE nº 2016/679.
[1908] G29, WP 243 rév. 01, Lignes directrices concernant les délégués à la protection des données (DPD), 5 avr. 2017, p. 14.
[1909] Sur le besoin de transdisciplinarité, v. *supra*, nº 490.
[1910] Selon une enquête menée par le Ministère du Travail, les profils de délégués à la protection des données se diversifient puisque 7 % d'entre eux sont issus des domaines liés à la qualité, la conformité et l'audit ; 13 % sont issus de domaines liés à l'administratif, aux finances et à la comptabilité ; 28 % sont issus du domaine juridique ; 29 % proviennent du domaine de l'informatique et 23 % sont dans d'autres domaines, v. Ministère du Travail, de l'Emploi et de l'Insertion, « Le métier de délégué à la protection des données (DPO) », enquête réalisée en mars et avril 2020, p. 5.
[1911] CNIL, *Rapport d'activité 2015,* La Documentation française, 2016, p. 47.
[1912] CNIL, *Rapport d'activité 2015,* La Documentation française, 2016, p. 47.

de délégué trouve une place de plus en plus importante au sein des organismes[1913]. L'impact réel du délégué à la protection sur l'effectivité de la protection des personnes demeure difficile à mesurer. Il est certain que pour la CNIL, la nomination d'un délégué apporte une illusion de conformité.

Ces limites intrinsèques à la fonction du délégué à la protection des données prouvent qu'il ne peut être la seule personne, au sein d'un organisme, à veiller au respect du droit des données personnelles.

B. Les experts techniques

499. La responsabilité des praticiens des données. Beaucoup des mesures prévues par le règlement européen, telles que les « mesures techniques et opérationnelles appropriées » ainsi que le principe de *privacy by design*[1914]*,* seront déterminées et mises en œuvre par les développeurs, les architectes logiciels, les *data scientists*, les administrateurs systèmes, les responsables de la sécurité et plus largement les ingénieurs employés par le responsable du traitement ou le sous-traitant. Ces personnes occupent donc un rôle au moins aussi important pour la mise en œuvre de la protection des personnes que celui du délégué à la protection des données personnelles[1915]. D'ailleurs, les informaticiens ont, depuis les balbutiements de l'informatique, alerté les législateurs sur le besoin de règles effectives pour la protection des personnes[1916]. Il semble donc naturel de considérer qu'ils ont, dans le cadre de leur travail, en plus de leurs obligations juridiques, une forme d'obligation morale. L'engagement de ces personnes à respecter une charte éthique pourrait donc être une voie à explorer[1917].

500. Une charte éthique. En 1974, le rapport Tricot s'était déjà interrogé sur l'opportunité de reconnaître un code de déontologie et un ordre pour les

---

[1913] Ministère du Travail, de l'Emploi et de l'Insertion, « Le métier de délégué à la protection des données (DPO) », enquête réalisée en mars-avril 2020, p. 9

[1914] CEPD, Avis 5/2018, avis préliminaire sur le respect de la vie privée dès la conception, 31 mai 2018 ; et le projet de lignes directrices sur ce sujet soumis à consultation, v. CEPD, Guidelines 4/2019 on article 25. Data protection by design and by default, 13 nov. 2019.

[1915] Sur l'importance du code informatique dans la protection des personnes, v. l'article fondamental de Monsieur Lawrence Lessig, L. Lessig, « Code is law. On liberty in cyberspace », *Harvard Magazine* janv. 2000.

[1916] Dès le début des années 1960, les risques liés à l'expansion de la collecte de données ont été présentés par des ingénieurs en informatique, v. A. Westin, *Privacy and Freedom*, Ig Publishing, 1968, réimpr. 2015, p. 334 ; G. González Fuster, *The emergence of personal data protection as a fundamental right of the EU*, Springer, 2014, p. 29 et F. Lane, *American privacy : the 400-year history of our most contested right*, Beacon Press, 2009, p. 144 s. V. aussi la vision de Bernard Benson et Richard Hamming, *supra*, nº 173.

[1917] Cathy O'Neil explique qu'un serment éthique pourrait être un des moyens, combiné avec d'autres, pour réguler les modèles algorithmiques, v. C. O'Neil, *Weapons of math destruction. How big data increases inequality and threatens democracy*, Crown New York, 2016, p. 205.

informaticiens[1918]. Le rapport avait écarté l'idée pour deux raisons : le caractère « trop récent et trop mouvant » de ce qui touche à l'informatique et la disparité des catégories professionnelles qui se rencontrent dans ce domaine. Depuis, le domaine a évolué et la première de ces justifications ne se vérifie plus tout à fait. Si les évolutions de l'informatique existent encore, elles sont d'une moindre ampleur et le domaine repose sur des principes connus. La seconde justification, à savoir la variété des professions, se vérifie toujours. Pour autant, cette raison doit être largement relativisé. En effet, il n'est pas nécessaire d'imposer à l'ensemble du secteur informatique une charte déontologique. Pour être efficace, cette dernière doit être réservée à certaines de ses professions.

Plusieurs organisations ont proposé d'instaurer des codes de bonnes pratiques déontologiques à l'adresse des développeurs et acteurs impliqués dans les traitements de données[1919]. Par exemple, sur le modèle du serment d'Hippocrate, l'association française Data for Good a proposé le « Serment d'Hippocrate pour Data Scientist ou pour toute personne travaillant avec la donnée »[1920]. Cette charte n'est pas le premier instrument de droit souple avancé appelant à une telle responsabilité éthique puisque, déjà en 1969, le philosophe Karl Popper plaidait pour « conserver, chez tous les scientifiques, la conscience de leur responsabilité »[1921] et que d'autres serments de ce type ont été proposés[1922]. Reconnaître l'application de principes éthiques aux professionnels de la donnée les encouragerait sans doute à prendre davantage en compte les effets des traitements, à s'impliquer dans la protection des personnes, et leur donnerait une plus grande force au sein des organismes. Dans plusieurs universités, les maquettes des formations d'ingénieurs incluent des cours dédiés aux questions d'éthique liées au développement de logiciels et à la mise en œuvre d'algorithmes[1923]. L'éthique est donc un complément aux principes juridiques.

[1918] B. Tricot, « Rapport de la commission Informatique et libertés », La Documentation française, 1975, p. 66.
[1919] C. Castets-Renard, « Comment construire une intelligence artificielle responsable et inclusive ? », *D.* 2020, p. 225.
[1920] Lors de la quatrième session d'accélération de l'association Data for Good, une équipe de bénévoles a proposé de rédiger un serment fondé sur cinq principes et une liste d'engagements afin de garantir l'intégrité et l'éthique des personnes travaillant avec les données.
[1921] K. Popper, « The moral responsibility of the scientist », *Encounter* mars 1969, p. 53.
[1922] Des organisations ont proposé ce type de serments, v. not. Association for Computing Machinery, « ACM code of ethics and professional conduct », 22 juin 2018.
[1923] Par exemple, plusieurs universités développent, au sein du département d'informatique, des programmes incluant des cours liés aux questions éthiques, v. not. T. Abate, « How the computer science department is teaching ethics to its students », *stanford.edu* 20 août 2020 ; P. Karoof, « Embedding ethics in computer science curriculum », *harvard.edu* 25 janv. 2019. De nombreuses autres universités, telles que Georgia Tech, le MIT ou l'EPFL proposent des cours d'éthique à leurs étudiants.

En plus de ces contrôles internes, des collaborations entre la CNIL et des experts participent aussi à renforcer l'efficacité des contrôles.

§ II. Le renforcement des contrôles résultant de coopérations

501. Des moyens restreints. Les moyens limités accordés aux autorités de contrôle à travers l'Europe brident l'ampleur de leurs actions[1924]. Celles-ci doivent choisir minutieusement leurs dossiers pour optimiser leur utilité et leur impact. En France, la CNIL effectue un nombre réduit de contrôles[1925] et prononce un nombre modique de sanctions pécuniaires[1926]. Selon elle, ces chiffres s'expliquent par sa fonction pédagogique qui vise à accompagner la conformité plutôt qu'à sanctionner les manquements[1927]. Pourtant, comme le remarquait à juste titre Monsieur Émile Gabrié, chef du service des affaires régaliennes de la CNIL, c'est en matière de sanctions que se joue sans doute la crédibilité des pouvoirs des autorités[1928].

502. Plan. Les ressources budgétaires de l'autorité de contrôle étant limitées, l'un des moyens d'amplifier son action est de s'ouvrir. C'est pourquoi des collaborations institutionnelles (A) ainsi qu'avec la société civile (B) se développent. À ces coopérations nationales s'ajoutent également des partenariats au niveau international (C).

A. Les coopérations institutionnelles

503. Le développement d'actions communes entre institutions. La CNIL renforce ses liens et coopérations avec certaines administrations ou autorités sur des compétences connexes, notamment dans le but de mutualiser les actions et protéger plus efficacement les personnes. Depuis 2011, la CNIL coopère ainsi avec la Direction Générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), l'autorité française chargée de la protection du consommateur[1929]. Elles

---

[1924] Brave, « Europe's governments are failing the GDPR », avr. 2020.
[1925] En moyenne, environ trois cents contrôles par année, v. Annexe 1 – Contrôles et sanctions de la CNIL.
[1926] En moyenne, moins de sept sanctions pécuniaires par année, v. Annexe 1 – Contrôles et sanctions de la CNIL.
[1927] M. Vivant, « L'État de non-droit », *D.* 2019, p. 753 ; v. aussi F. Mattatia, *RGPD et droit des données personnelles,* 4e éd., Eyrolles, 2019, p. 255 s.
[1928] É. Gabrié, « Les pouvoirs des autorités de protection des données », *Dalloz IP/IT* 2017, p. 268.
[1929] CNIL et DGCCRF, « Protocole général de coopération entre la Commission Nationale de l'Informatique et des Libertés et la Direction Générale de la concurrence, de la consommation et de la répression des fraudes », 6 janv. 2011.

ont notamment collaboré sur les traitements de données personnelles effectués par les réseaux sociaux ou les pratiques trompeuses liées à la mise en conformité au règlement européen[1930]. En janvier 2019, elles ont mis à jour leur convention de coopération pour l'adapter aux nouveaux enjeux du numérique[1931]. Ce nouveau protocole leur permet de réaliser des contrôles communs, de mutualiser leurs expertises et de proposer des évolutions du cadre législatif et réglementaire ou des actions au niveau européen.

De manière plus ponctuelle, la CNIL collabore également avec l'Agence nationale pour la sécurité des systèmes d'information (ANSSI). Par exemple, à la suite d'une coopération entre les deux institutions, le référentiel SecNumCloud lié à la qualification de prestataires de services d'informatique en nuage (*Cloud*) inclut désormais des exigences relatives à la protection des données[1932]. Cette coopération est très opportune parce que le domaine de la sécurité informatique est essentiel pour garantir la protection des données, comme en témoigne le nombre croissant de plaintes reçues par la CNIL sur ce sujet[1933].

Depuis 2018, la CNIL s'est également rapprochée de la Commission des clauses abusives. Ce rapprochement faisait suite au constat de l'insertion, de plus en plus fréquente, de clauses relatives aux données personnelles pouvant être de nature à créer un déséquilibre significatif au détriment des consommateurs[1934]. Pour l'instant, ce rapprochement demeure plutôt de nature informelle puisqu'il se matérialise surtout par des rencontres et des discussions entre les institutions. Ces discussions devraient aboutir *in fine* à des actions coordonnées tant le nombre de clauses abusives se glissant dans les conditions générales d'utilisation des grandes entreprises du numérique, telles que Twitter[1935], Google[1936] ou Facebook[1937], est important. D'autres rapprochements, notamment avec l'Autorité de Contrôle Prudentiel et de Résolution dans le domaine bancaire et de l'assurance, semblent également opportuns.

Ainsi, la CNIL a développé des partenariats pour atteindre un public plus large, pour mieux conseiller les organisations et, dans certains cas, pour mener des contrôles

---

[1930] CNIL et DGCCRF, « Pratiques abusives "Mise en conformité RGPD" : comment s'en prémunir avec la CNIL et la DGCCRF ? », 7 nov. 2018.
[1931] CNIL et DGCCRF, « La CNIL et la DGCCRF font évoluer leur protocole de coopération pour renforcer la protection des consommateurs et leurs données personnelles », 31 janv. 2019.
[1932] ANSSI, « SecNumCloud évolue et passe à l'heure du RGPD ».
[1933] Le rapport de la CNIL de 2018 indique d'ailleurs, sur la base des plaintes reçues par l'institution, que la sécurité des données personnelles est une préoccupation croissante des personnes concernées, v. CNIL, *Rapport d'activité 2018*, La Documentation française, 2019, p. 45.
[1934] Commission des clauses abusives, *Rapport annuel 2018,* p. 3.
[1935] TGI Paris, 7 août 2018, *UFC-Que Choisir* c. *Twitter*, nº 14/07300.
[1936] TGI Paris, 12 févr. 2019, *UFC-Que Choisir* c. *Google,* nº 14/07224.
[1937] TGI Paris, 9 avr. 2019, *UFC-Que Choisir* c. *Facebook*, nº 14/07928.

communs[1938]. À ces collaborations doivent également s'ajouter des coopérations avec la société civile.

B. Les coopérations avec la société civile

504. Des collaborations avec les institutions d'enseignement supérieur et de recherche. Puisqu'un faible taux des agents de la CNIL a des compétences techniques, il semble logique que des collaborations ou des rapprochements soient effectués sur certains projets entre la CNIL et des universités ou des écoles d'ingénieurs[1939]. Ce type de rapprochement existe déjà en Belgique où la Commission vie privée[1940] a fait appel à l'expertise technique des chercheurs de la *Katholieke Universiteit Leuven* et de la *Vrije Universiteit Brussel* (respectivement l'Université catholique flamande de Louvain et l'Université libre flamande de Bruxelles) afin de montrer les traçages illicites effectués par Facebook par le biais de technologies telles que les cookies, modules sociaux et pixels[1941].

De telles collaborations entre universitaires et autorités de protection doivent être encouragées[1942]. Elles favorisent la diffusion et l'utilisation des travaux de recherche, tout en apportant une aide technique salutaire aux agents des autorités.

505. Favoriser les divulgations responsables. À juste titre, le règlement européen a placé le principe de sécurité des traitements au cœur du dispositif de protection des données personnelles. En effet, ce texte impose aux responsables du traitement et aux sous-traitants de mettre en œuvre « les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque »[1943]. Ces mesures

---

[1938] La CNIL a également publié, avec l'ordre des médecins, un guide pratique à l'attention des médecins, v. CNIL et CNOM, « Guide pratique sur la protection des données personnelles », juin 2018. La CNIL a aussi publié avec la Banque Publique d'Investissement (Bpifrance) un guide pratique adapté aux très petites entreprises et aux petites et moyennes entreprises, v. CNIL et BPI, « Guide de sensibilisation au RGPD pour les petites et moyennes entreprises », avr. 2018. Plus récemment, la CNIL a signé un partenariat avec le Médiateur des entreprises, v. CNIL et Médiateur des entreprises, « Le médiateur des entreprises et la CNIL s'associent pour résorber les différends dans les relations contractuelles », 16 sept. 2020.

[1939] La CNIL a entamé timidement un tel rapprochement en participant à la création de la chaire Valeurs et Politiques des Informations Personnelles, animée par Madame Claire Levallois-Barth, au sein de l'Institut Mines Télécom.

[1940] Tribunal de première instance néerlandophone de Bruxelles, 16 févr. 2018, nº 2016/153/A, p. 4.

[1941] Pour rappel, les pixels sont des éléments de code logiciel placés sur une page web à l'intention des exploitants de sites web externes, permettant la collecte d'informations sur les visiteurs de ces pages.

[1942] Plusieurs universités, écoles ou instituts travaillent sur les enjeux de protection des données, tels que l'Institut national de recherche en sciences du numérique (INRIA) ou Télécom ParisTech.

[1943] Art. 32 du règlement UE nº 2016/679. La CNIL est relativement pointilleuse quant au respect de cette obligation, v. not. N. Métallinos, « Tolérance zéro de la CNIL en cas de manquement élémentaire à la sécurité », *CCE* 2019, nº 9, comm. 56 ; M. Griguer et S. Franco, « La CNIL durcit le ton en matière de sécurité. Étude comparative des sanctions prononcées à l'encontre des sociétés Uber et Bouygues Télécom », *Cahiers de droit de l'entreprise* 2019, nº 1, dossier 7.

visent à prévenir la survenance de violations de données personnelles, c'est-à-dire une violation de la sécurité, accidentelle ou illicite, entraînant la destruction, la perte, l'altération, la divulgation, ou l'accès non autorisé à de telles données[1944]. Ces violations de données peuvent avoir d'importantes répercussions sur les personnes[1945], notamment parce qu'elles facilitent les campagnes d'hameçonnage[1946] ou les usurpations d'identité[1947]. En plus des moyens internes pouvant être mis en œuvre par les organismes pour garantir la sécurité des données, d'autres mesures doivent être encouragées, telles que les « divulgations responsables ».

En sécurité informatique, la divulgation responsable correspond à un modèle de divulgation de vulnérabilité informatique selon lequel la personne ayant découvert une vulnérabilité laisse une période de temps à l'organisme pour la corriger avant de la rendre publique. Le système institutionnel est relativement peu enclin à protéger les auteurs de ces découvertes (souvent dénommés *hackers*)[1948]. Aux États-Unis par exemple, le *Computer Fraud and Abuse Act*[1949] a été invoqué dans de nombreuses affaires pour poursuivre et obtenir la condamnation de plusieurs *hackers* dans des affaires controversées[1950]. Le fait que ces *hackers* soient dans l'incapacité de divulguer ces failles de sécurité dans des conditions sereines a encouragé le développement d'un marché des failles de sécurité[1951].

Fort heureusement, la défiance à l'égard de ces chercheurs s'estompe progressivement pour laisser place à un système dans lequel les divulgations

---

[1944] Art. 4 § 12 du règlement UE nº 2016/679.

[1945] L'exploitation de vulnérabilités peut même résulter dans la propagation mondiale de virus informatiques. Par exemple, pendant plusieurs années, la NSA a exploité une vulnérabilité (Eternal Blue) présente dans le premier protocole SMB proposé par Microsoft. Quelques semaines après la révélation de cette vulnérabilité au public, les *ransomware* (virus bloquant l'ordinateur jusqu'au paiement d'une rançon) *WannaCry* et *NotPetya* se sont propagés mondialement. Sur ce sujet, v. J. Watkins, « No good deed goes unpunished : the duties held by malware researchers, penetration testers, and "white hat" hackers », *Minnesota Journal of Law, Science & Technology* 2018, vol. 19, p. 535 s. [19 MINN. J.L. SCI. & TECH. 535].

[1946] L'hameçonnage (ou *phishing* en anglais) est une technique consistant à faire croire à la victime qu'elle s'adresse à un tiers de confiance afin de lui soutirer des données personnelles.

[1947] Le considérant 85 du règlement UE nº 2016/679 affirme qu'une violation de données à caractère personnel risque de « causer aux personnes physiques concernées des dommages physiques, matériels ou un préjudice moral tels qu'une perte de contrôle sur leurs données à caractère personnel ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données à caractère personnel protégées par le secret professionnel ou tout autre dommage économique ou social important ».

[1948] Sur ce problème, v. not. l'affaire Bluetouff dans laquelle une administration avait poursuivi et obtenu la condamnation d'un journaliste qui avait récupéré des documents accessibles *via* un simple moteur de recherche du fait d'un défaut de sécurisation de l'extranet de l'administration, v. Cass. crim., 20 mai 2015, nº 14-81.336, *Bull. crim.* 2015, nº 119.

[1949] Pub. L. du 16 oct. 1986, nº 99-474, codifiée au 18 U.S.C. § 1030.

[1950] K. Zetter, « The most controversial hacking cases of the past decade », *Wired* 26 oct. 2015.

[1951] Par exemple, l'entreprise Zerodium est spécialisée dans l'achat de vulnérabilités informatiques, particulièrement les *Zero day* qui sont des vulnérabilités n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif déployé.

responsables sont possibles, voire encouragées. La loi pour une République numérique a, par exemple, organisé une protection juridique pour les personnes souhaitant informer l'ANSSI de l'existence d'une vulnérabilité[1952]. Cette protection reste malheureusement très minimaliste et ses conditions sont encore trop restrictives[1953]. D'ailleurs, la protection qui en résulte trouve d'importantes limites, comme le montre le récent licenciement par Deadalus d'un de ses employés lanceur d'alerte[1954]. Ce dernier avait alerté à plusieurs reprises son entreprise de l'existence d'une faille de sécurité exposant les données de 150 infrastructures médicales. Face à l'inaction de l'entreprise, il avait fini par informer l'ANSSI. Quelques semaines plus tard, le lanceur d'alerte était licencié pour faute grave. En France, une certaine défiance perdure donc à l'égard de ces personnes.

Aux États-Unis, le ministère de la Défense a ouvert, en 2016, le programme « Hack the Pentagon » encourageant des chercheurs en sécurité à trouver des vulnérabilités dans ses systèmes[1955]. Dans ce cadre, ce ministère a rémunéré plusieurs dizaines de *hackers* l'ayant informé de bugs et vulnérabilités passés sous les radars de ses agents. Les entreprises du secteur privé encouragent également ces pratiques en récompensant les personnes qui révèlent une vulnérabilité ou une faille dans la sécurité de leurs systèmes informatiques, *via* des programmes dénommés « *bug bounty* »[1956]. Puisque ces divulgations responsables évitent l'exploitation de failles de sécurité pouvant résulter ensuite dans du piratage d'informations, de l'espionnage ou de la surveillance, elles tendent à une meilleure protection des personnes et doivent donc être encouragées.

C. Les coopérations internationales

506. De nombreux textes internationaux. Le droit des données personnelles s'est d'abord construit au niveau national, en accompagnement du développement de l'informatique. L'arrivée d'Internet, réseau mondial décentralisé facilitant la

---

[1952] L'article 47 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique modifiant l'article L. 2321-4 du code de la défense a prévu que « L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée ».
[1953] Le statut de lanceur d'alerte devrait être renforcé, notamment pour permettre à des personnes constatant des violations de pouvoir les divulguer lorsque les mécanismes internes sont insuffisants. Sur le besoin de renforcer le statut de lanceur d'alerte, v. F. Chaltiel, *Les lanceurs d'alerte,* Dalloz, 2018, p. 99 s.
[1954] J.-M. Manach, « Un "leader européen" des données de santé licencie un lanceur d'alerte pour "faute grave" », *NextInpact* 2 oct. 2020.
[1955] The United States Digital Service, « Identifying security vulnerabilities in Department of Defense websites – Hack the Pentagon », *Report to Congress* 2016.
[1956] C'est Monsieur Jarrett Ridlinghafer qui a créé, en 1995, le premier programme *bug bounty* lorsqu'il était ingénieur chez Netscape Communications Corporation.

transmission d'informations au-delà des frontières, a très vite montré les limites de ces formes de règlementation[1957], encourageant ainsi l'adoption de standards internationaux[1958]. Pour éviter que la protection des données ou de la vie privée ne se cantonne à certains pays ou à certaines traditions juridiques, plusieurs instances supranationales ont introduit des principes liés à ces protections. En 1980 par exemple, le Conseil de l'OCDE a établi une recommandation régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel[1959]. Cette recommandation, révisée en 2013, instaure une approche liée à la gestion des risques, améliorant ainsi l'interopérabilité entre les législations, et favorisant la coopération entre les autorités de protection[1960]. En 1981, c'est le Conseil de l'Europe qui adoptait la Convention 108 avec l'objectif de protéger les droits de la personne face à la liberté internationale de circulation de l'information. Ce texte, amendé en 2018[1961], a trouvé un écho particulier en Europe grâce à son application par la CEDH[1962]. L'ONU a également participé à l'élaboration de principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel en établissant des garanties minimales applicables aux fichiers publics et privés[1963]. Pour la première fois, un instrument international recommandait la désignation d'une autorité de contrôle ayant pour mission d'assurer le respect des principes relatifs à la protection des données personnelles. En 2013, à la suite des révélations de Monsieur Edward Snowden[1964], l'ONU a adopté une nouvelle résolution pour réaffirmer la nécessité d'assurer une protection efficace de la vie privée à l'ère numérique[1965].

La Coopération économique pour l'Asie-Pacifique (APEC), qui compte vingt-et-un membres, dont les États-Unis, la Russie et la Chine, a également prévu un ensemble de règles transfrontalières. Le *Privacy Framework*[1966], adopté 2005, cherche

---

[1957] I. Falque-Pierrotin, « Rapport de la mission interministérielle sur l'Internet. "Internet, enjeux juridiques" », La Documentation française, 1997, p. 25 s.
[1958] J. Michael, *Privacy and Human Rights, an international and comparative study, with special reference to developments in information technology*, Unesco, 1994, p. 17.
[1959] OCDE, Lignes directrices du 23 sept. 1980 sur la vie privée et les flux transfrontières de données à caractère personnel.
[1960] OCDE, *Privacy framework*, 2013, p. 4.
[1961] Conseil de l'Europe, Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 18 mai 2018.
[1962] V. *supra*, nº 213.
[1963] ONU, Résolution nº 45/95, « Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel », 14 déc. 1990. Le rapporteur de ces lignes était le Français Louis Joinet, l'un des auteurs du Rapport Tricot, qui avait largement participé à l'adoption et à la mise en œuvre de la loi Informatique et libertés.
[1964] Rapport soumis au Conseil des droits de l'homme de l'ONU, « National security surveillance and human rights in a digital age », Brennan Center for justice, Access, ACLU, CDT, EFF, EPIC, HRW, Pen America, 2015.
[1965] ONU, Résolution nº 68/167, « Le droit à la vie privée à l'ère du numérique », 18 déc. 2013.
[1966] APEC, *Privacy framework*, 2005.

un équilibre entre la protection de la *privacy* et le développement du commerce électronique[1967]. Pour favoriser son application et son respect, l'APEC a créé le *Data Privacy Pathfinder*[1968].

L'abondance et la variété de ces textes et instances laisseraient penser qu'une protection efficace des données existe au niveau supranational. Pourtant, la plupart de ces textes ne sont pas appliqués, notamment à cause de leur caractère non contraignant et de l'absence d'autorité supranationale chargée de vérifier leur mise en œuvre[1969].

507. Des forums supranationaux coordonnant les actions des autorités nationales. En dépit de l'absence d'autorité supranationale chargée de garantir le respect des principes de protection des données, les autorités nationales coordonnent leurs actions dans plusieurs forums[1970]. Par exemple, la Conférence internationale des commissaires à la protection des données réunit chaque année plus d'une centaine d'autorités de protection des données issues du monde entier[1971]. L'objectif de cette conférence est de favoriser l'échange d'informations et d'élaborer des recommandations[1972]. Leur caractère non contraignant atténue toutefois largement leur influence. L'intérêt de ces réunions réside donc principalement dans le rassemblement, au sein d'une même enceinte, des autorités chargées de la mise en œuvre du droit des données personnelles[1973]. Cette conférence a facilité la création d'autres groupements, tels que le Groupe de Berlin[1974] ou l'Association francophone des autorités de protection des données personnelles[1975]. À nouveau, le caractère non contraignant des instruments adoptés par ces entités et le caractère ponctuel de ces rassemblements atténuent largement leur impact sur la protection des personnes.

Le *Global Privacy Enforcement Network* (GPEN), c'est-à-dire le réseau international d'autorités de protection des données, mis en place par l'OCDE en 2007,

---

[1967] APEC, *Privacy framework*, 2005, § 1.
[1968] APEC, *Data privacy pathfinder*, 2007.
[1969] J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 274.
[1970] Pour une liste non exhaustive des forums de discussion sur la vie privée, v. OCDE, *Protection de la vie privée en ligne orientations politiques et pratiques de l'OCDE*, OECD publishing, 2003, p. 61 s.
[1971] V. la liste des membres pouvant assister aux réunions restreintes.
[1972] OCDE, *Protection de la vie privée en ligne orientations politiques et pratiques de l'OCDE*, OECD publishing, 2003, p. 62.
[1973] J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 281.
[1974] Le Groupe de Berlin a pour objectif d'améliorer la protection de la vie privée et des données dans le secteur des télécommunications.
[1975] L'Association francophone des autorités de protection des données personnelles vise à promouvoir la protection des données personnelles, le renforcement des capacités de ses membres et le rayonnement de la vision et de l'expertise francophones à l'international, v. le site de l'AFADPD.

regroupe une cinquantaine d'autorités de contrôle d'Europe, d'Amérique du Nord et d'Amérique latine, d'Asie et du Pacifique[1976]. Il vise à renforcer la coopération sur les problèmes récurrents dans la mise en œuvre de la protection des données[1977]. Malgré l'adoption, en 2013, d'un plan d'action[1978], l'impact de ce réseau demeure relatif. L'une de ses actions, le *Internet Sweep day,* présente toutefois l'avantage de coordonner l'action des autorités autour d'une problématique commune : pendant une journée, les autorités membres du GPEN mènent une action conjointe pour auditer une pratique ou un secteur d'activité[1979]. Cette opération dresse ensuite un panorama international des tendances d'un secteur[1980].

La coopération supranationale se limite donc à des textes non contraignants et à des actions disparates aux effets relatifs pour la protection des données. Même au niveau européen, la coopération entre les autorités peine à exister.

508. La promesse déçue de l'autorité chef de file. Qualifiée de « révolutionnaire » par certains auteurs, la nouvelle gouvernance des autorités de contrôle organisée par le règlement européen met en œuvre de nouveaux mécanismes de coopération et d'assistance[1981]. C'est surtout la création du mécanisme de l'autorité chef de file qui est l'une des innovations les plus conséquentes de ce texte[1982]. En principe, l'autorité chef de file est compétente en cas de traitement transfrontalier de données à caractère personnel[1983], c'est-à-dire lorsqu'un traitement est effectué entre plusieurs États membres ou qu'il affecte sensiblement des personnes situées dans plusieurs États[1984]. Cette procédure de « guichet unique » désigne une autorité chef de file pour éviter à

[1976] V. la liste des autorités représentées dans le *Global Privacy Enforcement Network*.
[1977] OECD, « Recommendation on cross-border co-operation in the enforcement of laws protecting privacy », 2007, p. 5.
[1978] OECD, « Action Plan for the Global Privacy Enforcement Network (GPEN) », adopté le 15 juin 2012 et modifié le 22 janv. 2013.
[1979] V. par ex., CNIL, « Sweep day 2017 : des sites web et applications mobiles trop vagues sur l'utilisation des données personnelles ? », 24 oct. 2017 ; CNIL, « "Sweep 2018" : premières tendances sur la responsabilisation des sous-traitants informatiques à l'heure du RGPD », 5 mars 2019.
[1980] Pour une brève présentation de ces opérations conjointes, v. O. Tambou, « L'émergence d'un modèle européen d'interrégulation en matière de protection des données personnelles », *Mélanges J. Monéger*, 2017, LexisNexis, p. 382 s., spéc. p. 391. Sur les conséquences de l'audit réalisé en 2017 par le GPEN, v. Lamy, « Utilisation des données personnelles : audit par le GPEN des sites web et les applications mobiles », *RLDI* 2017, nº 142, p. 43.
[1981] J. Deroulez, « Les autorités de contrôle en droit des données personnelles », *CCE* 2018, nº 4, dossier 7. Madame Nathalie Martial-Braz était plus prudente quant à l'efficacité de ces actions, N. Martial-Braz, « L'extraterritorialité des décisions des autorités de régulation nationales : gage d'efficacité de la protection des données personnelles », *RUE* 2016, p. 288.
[1982] Pour une étude des innovations du règlement européen en matière d'autorités de contrôle, v. not. J. Deroulez, « Les autorités de contrôles en droit des données personnelles », *CCE* 2018, nº 4, dossier 7.
[1983] Art. 56 du règlement UE nº 679/2016.
[1984] Art. 4 § 23 du règlement UE nº 679/2016. Sur l'interprétation de cette notion, v. G29, WP 244 rév. 01, Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable de traitement ou d'un sous-traitant, 5 avr. 2017, p. 5.

ces organismes de devoir interagir avec plusieurs autorités nationales sur une même affaire. Pour bénéficier de cette procédure, l'organisme doit avoir un seul établissement sur le territoire européen ou y désigner un établissement principal[1985]. L'autorité chef de file ouvre et mène l'enquête en coopérant avec les autres autorités concernées pour réussir à parvenir à un consensus[1986]. L'objectif de ce guichet unique est donc de mutualiser les enquêtes et de garantir une application uniforme des règles européennes[1987].

En pratique, la mise en œuvre concrète de cette procédure a rencontré de nombreux obstacles. Tout d'abord, malgré les intentions louables du législateur européen d'uniformiser le droit de la protection des données personnelles, la profusion de renvois opérés par le règlement européen génère une fragmentation préjudiciable[1988]. Celle-ci rend la tâche des autorités chefs de file plus complexe puisqu'elles doivent jongler entre plusieurs implémentations différentes des règles issues du règlement européen.

Par ailleurs, et comme certains auteurs l'avaient prédit, l'existence du guichet unique favorise le *forum shopping,* en autorisant l'installation des organismes dans les États membres dont les autorités de contrôle sont les plus allantes[1989]. Ainsi, la plupart des grandes entreprises du numérique américaines ont établi leur établissement principal ou leur établissement unique en Irlande (Google, Facebook, Dell, LinkedIn ou encore Apple) ou au Luxembourg (Amazon). Les autorités irlandaise et luxembourgeoise sont donc chargées d'une part importante de la mise en œuvre

---

[1985] Sur l'interprétation de la notion d'établissement principal, v. G29, WP 244 rév. 01, Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable de traitement ou d'un sous-traitant, 5 avr. 2017, p. 5 s. V. not. L. Pailler, « L'applicabilité spatiale du Règlement général sur la protection des données (RGPD), commentaire de l'article 3 », *Journal du droit international* 2018, nº 3, doctr. 9 ; J.-P. Dom, « Matérialité et localisation de l'entreprise numérique », *Dalloz IP/IT* 2019, p. 661.

[1986] G29, WP 244 rév. 01, Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable de traitement ou d'un sous-traitant, 5 avr. 2017, p. 10.

[1987] Pour une étude sur la coopération entre les autorités, v. E. Brunet, « Les mécanismes de coopération des autorités de contrôle au sein de l'Union européenne et le Comité européen de la protection des données », *Revue de Droit International d'Assas* 2019, nº 2, p. 117.

[1988] Le règlement européen effectue 56 renvois aux droits nationaux, v. A.-Y. Le Dain et P. Gosselin, « Rapport d'information sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française », Assemblée nationale, nº 4544, 22 févr. 2017, annexe nº 1.

[1989] V. déjà N. Martial-Braz, J. Rochfeld et E. Gattone, « Quel avenir pour la protection des données à caractère personnel en Europe ? Les enjeux de l'élaboration chaotique du règlement 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 », *D.* 2013, p. 2788. V. aussi, N. Métallinos, « Les leçons à tirer de la sanction de Google par la CNIL (1re partie : pas de « guichet unique » pour Google !) », *CCE* 2019, nº 5, comm. 35. D'ailleurs, les lignes directrices concernant la désignation d'une autorité de contrôle chef de file ont identifié ce problème, v. G29, WP 244 rév. 01, Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable de traitement ou d'un sous-traitant, 5 avr. 2017, p. 9.

européenne du droit des données à caractère personnel[1990]. Pourtant, après deux années d'application du règlement européen, ces autorités ont entamé de nombreuses enquêtes qui n'ont abouti, à ce jour, à pratiquement aucune sanction[1991]. Le système de guichet unique fait donc l'objet de véhémentes critiques provenant tant de la part de la société civile[1992] que des autres autorités de contrôle qui sont soumises au rythme imposé par ces autorités chefs de file[1993]. Même le ton feutré de la Commission européenne s'est raffermi face aux complications liées à la mise en œuvre du guichet unique. Elle a appelé de ses vœux des avancées « en vue d'un traitement plus efficace et davantage harmonisé des situations transfrontières dans l'ensemble de l'UE, y compris sur le plan procédural, pour des aspects tels que les procédures de traitement des plaintes, les critères de recevabilité des plaintes, la durée des procédures due à des différences de délais ou à l'absence de délais dans les législations nationales en matière de procédure administrative »[1994]. L'engorgement actuel du système de guichet unique était prévisible, et il convient donc de trouver des moyens pour éviter que le respect aux règles du droit des données personnelles reste si peu contrôlé.

509. Conclusion de chapitre. Une meilleure mise en œuvre du droit des données personnelles passe nécessairement par un renforcement des contrôles. Ces contrôles encouragent les organismes à investir des moyens humains et matériels dans la protection des données personnelles.

Au niveau des contrôles administratifs, pour renforcer la légitimité de la CNIL et prévenir les risques de conflits d'intérêts, les règles applicables à ses services doivent s'inspirer de celles auxquelles sont soumis les membres du collège. Par ailleurs, les garanties procédurales devant l'autorité doivent être consolidées, notamment pour renforcer la transparence de son travail. Cette transparence serait bénéfique pour les

---

[1990] Dès lors que le contentieux concerne « un traitement transfrontalier » effectué par le responsable du traitement ou le sous-traitant, au sens de l'article 56 du règlement UE nº 2016/679.
[1991] V. Federprivacy, « 2019 statistical report of privacy sanctions in Europe », *Federprivacy* 10 janv. 2020. D'ailleurs, le rapport d'activité de la Commission irlandaise de protection des données montre un nombre important d'enquêtes ouvertes mais peu de résultats, DPC, « DPC Ireland 2018 –2020. Regulatory activity under GDPR ».
[1992] V. par ex. Access Now, « Two years under the EU GDPR. An implementation progress report », mai 2020 ; NYOB, « Open letter », 25 mai 2020.
[1993] N. Vinocur, « "We have a huge problem" : European tech regulator despairs over lack of enforcement », *Politico* 27 déc. 2019 ; D. Scally, « German regulator says Irish data protection commission is being overwhelmed », *The Irish Times* 3 févr. 2020.
[1994] Commission, COM2020 264, « Communication de la Commission au Parlement européen et au Conseil. La protection des données : un pilier de l'autonomisation des citoyens et de l'approche de l'Union à l'égard de la transition numérique – deux années d'application du règlement général sur la protection des données », 24 juin 2020, p. 6.

auteurs de réclamations et pour le grand public. Enfin, l'autorité doit accélérer sa transformation en diversifiant les profils de ses agents et de ses commissaires. De telles mesures renforceront la confiance dans l'institution et la légitimité de son action.

D'autres formes de contrôle viennent épauler l'action de l'autorité. Au sein des organismes traitant des données, plusieurs personnes peuvent contribuer à garantir le respect de la protection des personnes. Le délégué à la protection des données et les professionnels des traitements de données participent indéniablement à une mise en œuvre du droit plus respectueuse des personnes. À ce titre, l'élaboration d'une charte éthique destinée à ces personnes s'avère une voie intéressante à explorer.

En plus de ces contrôles internes, les contrôles externes se développent. Ils se matérialisent par des collaborations institutionnelles valorisant la mutualisation des ressources et prennent la forme de partenariats, notamment avec des institutions de recherche. Les coopérations internationales demeurent confrontées à d'importantes difficultés et leur impact concret pour la protection des personnes reste, à ce jour, très relatif. À ces contrôles opérés par les acteurs spécialisés s'ajoute également la place de la réalisation juridictionnelle de cette matière.

Chapitre II – La réalisation juridictionnelle

510. La réalisation du droit. Pour Henri Motulsky, « le droit est fait pour la réalisation journalière dans les cas d'espèce »[1995] et il « n'atteint sa plénitude qu'en se réalisant »[1996]. Ainsi, l'affirmation des droits n'est que peu de chose en l'absence de leur mise en œuvre concrète. En référence à la formule de Jhering, la réalisation du droit est la vie et la vérité du droit[1997]. Sonder la question de l'effectivité d'un droit ou d'une protection pousse inévitablement à l'étude de sa réalisation. D'ailleurs, le verbe « réaliser » renvoie directement à cette idée puisqu'il se définit comme le fait de « rendre réel, effectif »[1998]. À ce titre, l'ineffectivité serait une des pathologies de la réalisation du droit[1999].

511. La réalisation juridictionnelle. Il est classique de distinguer la réalisation non contentieuse de la réalisation contentieuse[2000]. Fort heureusement, la première est celle qui s'accomplit le plus souvent[2001]. En effet, la plupart du temps, les comportements adoptés par les destinataires de la règle de droit s'accordent avec ses exigences, et les droits reconnus sont donc exercés sans difficulté. Il arrive toutefois que la règle entraîne des comportements non désirés, en décalage avec les objectifs poursuivis[2002]. En conséquence, le titulaire d'un droit doit pouvoir le faire respecter et faire sanctionner les atteintes qui pourraient y être portées. Cette sanction passe par une action en justice dont l'exercice donne lieu à un procès.

512. La protection contentieuse des données personnelles. L'utilisation du numérique dans tous les pans de nos vies a suscité une prise de conscience généralisée de l'ampleur des risques que les traitements de données font peser sur les personnes et la société. La nature des atteintes provoquées par ces traitements ainsi que leurs effets

---

[1995] P. Roubier, « Préface » à la thèse de Henri Motulsky, *Principes d'une réalisation méthodique du droit privé. La théorie des éléments générateurs des droits subjectifs*, th. Lyon, 1948, réimpr. Dalloz, 2002, p. IX.
[1996] H. Motulsky, *Principes d'une réalisation méthodique du droit privé. La théorie des éléments générateurs des droits subjectifs*, th. Lyon, 1948, réimpr. Dalloz, 2002, n° 150, p. 174.
[1997] F. Leborgne, « Le droit selon Henri Motulsky », *Revue juridique de l'Ouest* 2015, n° 2, p. 9, spéc. p. 12.
[1998] *Dictionnaire de l'Académie française*, 9e éd., *V°* « Réaliser », sens 1.
[1999] Messieurs François Terré et Nicolas Molfessis étudient la question de l'effectivité d'un droit dans la perspective de sa réalisation, v. F. Terré et N. Molfessis, *Introduction générale au droit*, 11e éd., Dalloz, 2019, nos 581 s., p. 659 s.
[2000] P. Malinvaud, *Introduction à l'étude du droit*, 20e éd., LexisNexis, 2020, n° 478 et n° 479, p. 433 s.
[2001] P. Malinvaud, *Introduction à l'étude du droit*, 20e éd., LexisNexis, 2020, n° 478, p. 433 ; F. Terré et N. Molfessis, *Introduction générale au droit*, 11e éd., Dalloz, 2019, n° 580, p. 658.
[2002] F. Terré et N. Molfessis, *Introduction générale au droit*, 11e éd., Dalloz, 2019, n° 581, p. 659.

ont mis en exergue la nécessité d'assurer une protection effective des données personnelles. Au départ principalement préventif, le droit des données personnelles est aujourd'hui un droit répressif[2003]. L'organisation du contentieux de cette matière ne ressemble à aucune autre puisque ses règles s'appliquent de manière transversale et commandent une répartition des recours entre les deux ordres de juridictions. Quelles sont les conséquences d'une telle répartition des recours et quelle cohérence d'ensemble en ressort ?

513. La réparation des dommages engendrés par le manquement au droit des données personnelles. L'étude de ce contentieux amène à s'interroger sur son régime, et plus particulièrement sur le régime de responsabilité extracontractuelle érigé par le règlement européen. *A priori*, ce régime révèle plusieurs éléments de complexité, notamment en matière de preuves ainsi qu'en ce qui concerne l'évaluation du préjudice. La faible réalisation juridictionnelle amène à se demander si le régime actuel est adapté aux types d'atteintes et s'il encourage les victimes à agir pour s'assurer du respect de leurs droits.

514. Plan. Après avoir montré pourquoi il est nécessaire d'atténuer la pluralité de procédures (Section I), nous verrons qu'il faut aussi faciliter les actions en responsabilité (Section II).

SECTION I – ATTÉNUER LA PLURALITÉ DE PROCÉDURES

515. Les procédures. Pour garantir le respect des règles prévues par le droit des données personnelles, plusieurs procédures juridictionnelles sont possibles. Une telle pluralité de recours n'est-elle pas nuisible à l'intelligibilité et l'accessibilité de la réalisation du droit des données personnelles ? L'accomplissement de l'objectif d'une justice plus lisible et plus compréhensible pour les citoyens passe par l'amélioration de l'accès à celle-ci et invite donc à sa simplification[2004]. L'organisation des recours, telle qu'elle résulte des strates successives accumulées au fil des ans, laisse entrevoir une

[2003] Sur le passage d'un droit préventif à un droit répressif, v. *supra*, nº 309.
[2004] S. Guinchard, « Rapport au garde des Sceaux. L'ambition raisonnée d'une justice apaisée », La Documentation française, 2008, p. 247.

fragmentation des recours. Une telle fragmentation n'est-elle pas préjudiciable à la mise en œuvre des actions ?

516. Plan. La réalisation juridictionnelle du droit des données à caractère personnel s'illustre par des recours fragmentés (§ I) qu'il convient de canaliser (§ II).

§ I. Des recours fragmentés

517. Plan. L'étude des différents recours prévus par le droit des données dévoile un système encombré (A). De ce système se dégage une impression d'incohérence (B).

A. Variété des recours

518. Variété d'acteurs dans la mise en œuvre du droit des données personnelles. L'une des particularités du droit des données personnelles est qu'il transcende les balancements classiques connus par le droit français, notamment la dualité entre le droit public et le droit privé[2005]. Les mêmes règles sont applicables à la plupart des secteurs d'activité et des organismes traitant des données personnelles, qu'il s'agisse de personnes de droit public ou de droit privé[2006]. Dès lors, les acteurs impliqués dans la mise en œuvre du droit des données personnelles sont nombreux et hétéroclites. Au niveau national, au moins cinq acteurs peuvent être sollicités pour garantir le respect du droit des données personnelles. À ces acteurs nationaux s'ajoutent également les interventions de la CJUE[2007] ou de la CEDH[2008]. Notre étude se limitera à l'analyse de la réalisation juridictionnelle devant les acteurs nationaux, dès lors que c'est elle qui est la plus fréquente et qui pose le plus de difficultés.

519. Plan. L'étude des recours devant la CNIL (1) précèdera celle de ceux pouvant être formés devant le juge judiciaire (2) et le juge administratif (3).

[2005] P. Ancel, « La protection des données personnelles : aspects de droit privé français », *RID comp.* 1987, vol. 39, nº 3, p. 609, spéc. p. 611. V. aussi, J. Carbonnier, *Droit civil,* vol. 1, *Introduction. Les personnes. La famille, l'enfant, le couple*, PUF, 2004, nº 287 p. 535. Pour un panorama récent sur le dualisme juridictionnel, voir le dossier consacré à cette question par la Revue de droit d'Assas, « L'avenir du dualisme juridictionnel : continuité ou rupture ? », *Revue de droit d'Assas* 2019, nº 18, p. 32 s. Pour une présentation de la transdisciplinarité du droit des données à caractère personnel, v. *supra*, nº 9.

[2006] Pour une analyse relative à la répartition entre les deux ordres de juridiction, v. J. Massot, « La répartition entre les deux ordres », *RFDA* 2010, p. 907.

[2007] O. Tambou, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, nº 453, p. 393.

[2008] V. la fiche thématique proposée par l'unité de la presse de la CEDH sur la protection des données personnelles, v. CEDH, « Protection des données personnelles », Fiche thématique, mai 2020.

1. Les recours devant la CNIL

520. Les réclamations devant la CNIL. La CNIL s'empare d'une grande partie des recours des personnes concernées[2009] puisqu'elle peut être saisie dans le cadre d'une réclamation individuelle[2010], et par des recours collectifs[2011]. Comme cela a été développé, la réclamation n'a pas pour effet d'ouvrir un contentieux au nom de son auteur devant l'autorité[2012]. La CNIL procède à l'examen des faits à l'origine de cette réclamation et décide souverainement des suites à lui donner[2013]. Le caractère contentieux des réclamations ouvertes devant la CNIL pour les personnes concernées est donc assez limité.

2. Les recours devant le juge judiciaire

521. Les recours devant le juge pénal. Le code pénal consacre une section entière aux atteintes aux droits de la personne résultant des fichiers ou traitements informatiques, avec pas moins de quinze articles dédiés à ces infractions[2014]. Le ministère public et les victimes auraient donc pu y trouver un terreau fécond pour défendre les principes du droit des données à caractère personnel. Pourtant, le contentieux pénal se révèle plutôt rare[2015]. Souvent déploré par la doctrine[2016], le déséquilibre manifeste entre les nombreuses infractions et le faible contentieux s'explique notamment par un taux insignifiant de transmission des affaires par la CNIL au parquet[2017], et par l'intérêt relatif des enquêteurs pour ces formes d'atteintes aux personnes. Ainsi, le grand nombre d'infractions consacrées par le code pénal ne reflète

---

[2009] Selon Madame Olivia Tambou, ce choix serait fondé sur trois raisons principales : tout d'abord parce que le recours est gratuit, ensuite parce que la personne n'a pas à prouver la violation, et enfin parce qu'elle peut choisir l'autorité nationale de son choix, v. O. Tambou, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, p. 394.
[2010] Art. 77 du règlement UE nº 679/2016.
[2011] Art. 80 du règlement UE nº 679/2016 et sur le fondement de l'article 38 de la loi nº 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018.
[2012] V. *supra*, nº 486.
[2013] V. *supra*, nº 486.
[2014] Art. 226-16 s. du code pénal.
[2015] *JCP pénal code*, fasc. 20, « Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques », par A. Mihman, 2018, nºs 25 s. ; J. Frayssinet, « La régulation du respect de la loi Informatique, fichiers et libertés par le droit pénal : une épée de bois », *Légipresse* 2009, nº 42, p. 23 s.
[2016] D. Forest, « Propos intempestifs sur les recours juridictionnels concernant les données personnelles », *RLDI* 2020, nº 166, p. 38 ; J. Francillon, « Infractions relevant du droit de l'informatique. La loi Informatique, fichiers et libertés du 6 janvier 1978 à l'épreuve de la jurisprudence pénale », *RSC* 1996, p. 676 et A. Lepage, « Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », *CCE* 2005, nº 2, étude 9.
[2017] Entre 1978 et 2019, seules 48 dénonciations ont été transmises au parquet, soit un peu plus d'une par année, v. Annexe 2 – Dénonciations au parquet effectuées par la CNIL.

pas fidèlement la place du juge pénal dans la mise en œuvre de la protection des données personnelles, lequel occupe, depuis 1978, un rôle plutôt effacé.

522. Les recours devant le juge civil avant l'entrée en application du règlement européen. Pendant longtemps, le juge civil a eu un rôle modeste dans la réalisation du droit des données personnelles. En effet, jusqu'au milieu des années 2010, aucune voie de recours ne lui reconnaissait de compétence particulière[2018]. Certains fondements de la responsabilité civile, contractuelle[2019] et délictuelle[2020] auraient valablement pu être invoqués par les personnes concernées pour protéger leurs données personnelles devant le juge civil. En réalité, ces articles ont rarement été sollicités à cette fin. Plusieurs raisons peuvent expliquer ce faible contentieux. D'abord la technicité du droit des données personnelles a sans doute rebuté de nombreux plaideurs, d'autant que les règles sont relativement accommodantes pour les organismes et qu'ils en sont les principaux contrôleurs. À cela s'ajoutent également des difficultés pour prouver les manquements[2021]. Par exemple, comment le plaideur peut-il apporter la preuve du manquement à la confidentialité des données ou le détournement de finalité ? De plus, la mise en œuvre d'une telle action a sans doute été jugée trop complexe par rapport aux effets de l'atteinte engendrée par un simple traitement illicite de données personnelles[2022]. Seuls les traitements les plus intrusifs risquent de motiver une action en justice, puisque celle-ci a un coût élevé et requiert un engagement important pour les personnes[2023]. Enfin, les fondements classiques, et particulièrement celui relatif à la responsabilité civile délictuelle, sont peu adaptés aux atteintes causées par les traitements de données personnelles : les juges interprètent strictement les conditions

---

[2018] D'ailleurs, il est remarquable de constater qu'aucune mesure de transposition n'a été prise par le législateur français pour inclure, dans la loi Informatique et libertés, un fondement de responsabilité en cas de traitement illicite ou de manquement aux règles du droit des données personnelles. Dans son rapport, Guy Braibant appelait pourtant à l'adoption d'une telle mesure. Il rappelait l'importance de cette transposition dès lors que l'article 23 de la directive 95/46 crée « une présomption spéciale de responsabilité à la charge du "responsable du traitement" qui n'est pas incompatible avec notre droit, mais qui n'y figure pas actuellement », v. G. Braibant, « Données personnelles et société de l'information. Rapport au Premier ministre sur la transposition en droit français de la directive nº 95/46 », La Documentation française, 1998, p. 78.

[2019] Cette responsabilité est prévue aux nouveaux articles 1231 et suivants du code civil. Dans l'hypothèse où le fondement de licéité du traitement de données est le contrat, les relations entre la personne concernée et le responsable du traitement doivent être qualifiées de contractuelles. Les obligations du responsable du traitement auront donc, en principe, une nature contractuelle, et leur violation pourra déboucher sur une responsabilité de cette nature, v. sur ce point, E. Netter, « L'extinction du contrat et le sort des données personnelles », *AJ Contrat* 2019, p. 416 et A. Danis-Fatôme, « Quelles actions judiciaires en cas de violation du RGPD ? », *CCE* 2018, nº 4, dossier 18, § 8.

[2020] Ces types de responsabilité sont prévus à l'article 9 et aux nouveaux articles 1240 et 1241 du code civil.

[2021] V. *infra*, nºs 544 s.

[2022] Cela fait d'ailleurs écho à l'adage *de minimis non curat praetor* signifiant que le préteur ne doit pas s'occuper des causes insignifiantes.

[2023] V. *supra*, nº 215.

d'application, notamment celle de faute[2024] ou de préjudice, réduisant ainsi les chances de succès de telles actions[2025].

523. Les recours devant le juge civil après l'entrée en application du règlement européen. La réception en droit français du règlement européen a métamorphosé, en théorie au moins, la place du juge civil dans la mise en œuvre de la protection des données personnelles. Désormais, il est compétent pour recevoir des demandes individuelles et collectives. Aux recours individuels fondés sur la responsabilité civile de droit commun, l'article 82 du règlement européen ajoute un nouveau recours en responsabilité. Celui-ci reprend les trois conditions classiques de la responsabilité civile délictuelle (la faute, le préjudice et le lien de causalité) et permet d'obtenir la réparation du préjudice causé[2026].

En plus de ces recours individuels, les personnes concernées peuvent unir leur force et agir de manière coordonnée. En France, deux types d'action collective sont ainsi envisageables : d'une part, l'action de groupe, introduite par la loi du 18 novembre 2016 dite de « modernisation de la justice du XXIe siècle »[2027], et d'autre part, l'action en représentation collective. Cette dernière accorde aux personnes concernées le droit de mandater un organisme[2028] pour qu'il agisse en leur nom dans deux types de cas. Tout d'abord, l'organisme peut être mandaté pour former un recours collectif lorsque les personnes concernées estiment que leurs droits ont été violés du fait d'un manquement au droit des données personnelles[2029]. Dans cette hypothèse, le juge civil est saisi pour constater le manquement, et ce, même s'il n'en résulte pas de préjudice apparent. En pratique, une telle action risque de ne pas intéresser les plaideurs puisqu'elle vise principalement à obtenir la cessation de l'illicite. Le déséquilibre entre l'investissement requis et son résultat n'encourage pas les groupements à privilégier ce type de recours.

[2024] Cass. civ. 1re, 10 sept. 2014, nº 13-12.464, *Bull. civ.* 2014, I, nº 144. Sur l'obstacle empêchant de faire droit à une demande de rectification de nom patronymique, v. Cass. civ. 1re, 4 mai 2012, nº 10-27.208, *NPB*.
[2025] Sur les difficultés de mise en œuvre du droit au respect de la vie privée sur le fondement de la responsabilité civile extracontractuelle et le besoin d'adopter un fondement spécifique, v. *supra*, nº 321.
[2026] Pour une analyse de la mise en œuvre de ces conditions, v. *infra*, nos 544 s.
[2027] Loi nº 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle, *JORF* 19 nov. 2016, nº 0269, texte 1.
[2028] En vertu de l'article 38 de la loi nº 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance nº 2018-1125 du 12 déc. 2018, la personne concernée peut mandater « une association ou une organisation mentionnée au IV de l'article 37, une association ou une organisation dont l'objet statutaire est en relation avec la protection des droits et libertés lorsque ceux-ci sont méconnus dans le cadre d'un traitement de données à caractère personnel, ou une association dont cette personne est membre et dont l'objet statutaire implique la défense d'intérêts en relation avec les finalités du traitement litigieux ».
[2029] Art. 79 du règlement UE nº 679/2016.

En sus de cette action, un organisme peut également être mandaté par un groupe de personnes pour agir en réparation du préjudice subi à la suite d'un manquement au règlement européen[2030]. Cette action suppose la réunion préalable de mandats écrits, lesquels ne peuvent pas être sollicités par l'organisme[2031]. En pratique, ces actions se sont déjà révélées inefficaces dans d'autres domaines, notamment en droit de la consommation, alors même qu'elles existent depuis plusieurs années[2032]. Elles ne trouvent pas, pour l'instant, un écho plus favorable en droit des données à caractère personnel.

À ces actions en représentation conjointe s'ajoutent également deux actions de groupe. Un temps envisagé au niveau européen, le règlement a finalement renvoyé aux États membres la compétence de la prévoir dans leur droit interne, ce qui n'a pas manqué de générer une fragmentation territoriale préjudiciable[2033]. En France, cette action avait timidement été introduite par la loi du 18 novembre 2016, mais elle se limitait à la seule demande de cessation de l'illicite, encadrement qui n'a pas manqué d'être critiqué par la doctrine[2034]. Le législateur français a saisi l'opportunité de la réception en droit français du règlement européen pour étendre l'action de groupe aux demandes en réparation des dommages[2035]. Certains organismes[2036] sont désormais compétents pour former des recours en réparation devant le juge civil, lesquels doivent avoir été précédés d'une mise en demeure restée infructueuse pendant quatre mois[2037]. Lorsque l'action de groupe tend à la réparation des préjudices subis, trois phases successives conformes au régime de l'*opt-in* sont prévues :

(1) le juge statue sur la responsabilité du défendeur,

[2030] Art. 38 de la loi n° 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance n° 2018-1125 du 12 déc. 2018.
[2031] Contrairement à l'action de groupe, l'association a l'interdiction de faire usage de « tout appel public par moyen de communication de masse ou par lettre personnalisée », Cass. civ. 1re, 26 mai 2011, n° 10-15.676, *Bull. civ.* 2011, I, n° 98.
[2032] M. Bacache-Gibelli, *La responsabilité civile extracontractuelle,* 3e éd., Economica, 2016, n° 410, p. 481.
[2033] C. Zolynski, « Les nouveaux contours de l'action de groupe et de l'action collective au lendemain de la loi pour la protection des données : un *empowerment* renforcé », *Dalloz IP/IT* 2018, p. 470.
[2034] V. not. N. Métallinos, « Introduction d'une action de groupe en matière de violation de la loi Informatique et libertés », *CCE* 2016, n° 11, comm. 95 ; S. Amarani-Mekki, « Le socle commun procédural de l'action de groupe de la loi de modernisation de la justice du XXIe siècle. À propos de la loi n° 2016-1547 du 18 novembre 2016 », *JCP G* 2016, n° 50, p. 1340 ; A. Danis-Fatôme, « Quelles actions judiciaires en cas de violation du RGPD ? », *CCE* 2018, n° 4, dossier 18, § 21.
[2035] P. Forteza, « Rapport sur le projet de loi relatif à la protection des données personnelles », Assemblée nationale, n° 592, 25 janv. 2018, p. 27. Dans sa décision du 25 janvier 2018, la CJUE avait considéré que les principes de protection issus du droit européen reconnaissant un for du consommateur ne peuvent être invoqués que lorsque le consommateur est demandeur ou défendeur dans une procédure, CJUE, 25 janv. 2018, *Maximilian Schrems.* c. *Facebook Ireland Limited,* C-498/16, § 44 s.
[2036] L'article 37 IV de la loi n° 78-17 du 6 janvier 1978 telle que modifiée par l'ordonnance n° 2018-1125 du 12 déc. 2018, n'autorise que trois types de groupements à porter cette action : les associations déclarées depuis cinq ans dont l'objet est la protection de la vie privée ou des données personnelles, certaines associations de défense des consommateurs et certaines organisations syndicales ou représentatives.
[2037] Art. 63 de la loi n° 2016-1547 du 18 novembre 2016.

(2) avant de définir le groupe de personnes susceptibles de bénéficier de l'action de groupe,

(3) et enfin de fixer les délais permettant aux victimes d'adhérer au groupe[2038].

L'organisme condamné est alors tenu d'indemniser chacune de ces personnes. Ainsi, les personnes concernées peuvent rallier l'action de groupe lorsqu'elles sont sûres d'obtenir la réparation de leur préjudice. Cette montée en puissance du juge civil dans le contentieux du droit des données personnelles témoigne de la volonté des législateurs européen et français de rendre ce droit plus effectif et mieux respecté.

3. Les recours devant le juge administratif

524. Les recours devant le juge administratif. Si le législateur français n'a pas donné à la CNIL le pouvoir d'imposer des amendes administratives à l'État[2039], les juridictions administratives restent compétentes pour connaître des litiges liés aux traitements illicites effectués par celui-ci. Le tribunal administratif peut donc être saisi par un demandeur sur les fondements classiques de la responsabilité pour faute de l'administration[2040]. À ce droit de recours individuel s'ajoutent également les mêmes voies de recours collectifs que celles prévues en droit civil, c'est-à-dire les actions en représentation collective[2041], ainsi que les actions de groupe[2042].

525. Les recours devant le Conseil d'État. En tant que juridiction de droit commun, le Conseil d'État est compétent pour connaître des recours contre les décisions du tribunal administratif prononcées en dernier ressort ou contre les décisions des cours d'appel administratives[2043]. En plus de cette compétence classique, le Conseil d'État connaît également des recours pour excès de pouvoir et de pleine juridiction contre les décisions de la CNIL. Lorsqu'il est saisi des avis, recommandations et prises de

---

[2038] Art. 66 de la loi n° 2016-1547 du 18 novembre 2016. V. aussi C. Zolynski, « Les nouveaux contours de l'action de groupe et de l'action collective au lendemain de la loi pour la protection des données : un *empowerment* renforcé », *Dalloz IP/IT* 2018, p. 470.

[2039] Art. 20 § III 7 de la loi n° 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance n° 2018-1125 du 12 déc. 2018.

[2040] R. Chapus, *Droit administratif général*, t. 1, 15e éd., Montchrestien, 2001, n° 1521, p. 1383 s. ; P.-L. Frier et J. Petit, *Précis de droit administratif*, 5e éd., Montchrestien, 2008, n° 25, p. 18 s. Le tribunal administratif est le juge de droit commun du contentieux administratif, J. Waline, *Droit administratif,* 28e éd., Dalloz, 2020, n° 645, p. 717. D'ailleurs, le juge administratif s'est reconnu compétent, sur le fondement de l'article 9 du code civil, pour une atteinte à la vie privée imputée à une personne publique, v. CE Sec., 30 décembre 1998, *Sargos*, n° 153994, *Lebon* p. 515.

[2041] Art. 80 § 1 du règlement UE n° 679/2016 et art. 38 de la loi n° 78-17 du 6 janv. 1978 telle que modifiée par l'ordonnance n° 2018-1125 du 12 déc. 2018.

[2042] Art. 63 s. de la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle.

[2043] Art. L. 111-1 du code de justice administrative.

position de la CNIL[2044], le Conseil d'État statue dans le cadre d'un recours pour excès de pouvoir[2045]. En principe, la Haute juridiction administrative opère alors un contrôle restreint puisque sa censure ne porte que sur une erreur de fait ou de droit, une erreur manifeste d'appréciation ou un détournement de pouvoir[2046]. Toutefois, lorsque l'auteur du recours est une personne physique se fondant sur la méconnaissance d'un de ses droits, le contrôle effectué par le Conseil d'État sur la délibération de la CNIL est, dans ce cas, plus large[2047].

Quant aux sanctions prononcées par la CNIL, elles sont susceptibles de faire l'objet d'un recours de pleine juridiction devant le Conseil d'État. Suivant la définition classique de Laferrière, les pouvoirs de pleine juridiction comportent l'exercice d'un arbitrage complet, de fait et de droit, sur le litige[2048]. Le Conseil d'État se prononce alors comme les tribunaux ordinaires entre deux parties litigantes : la Haute juridiction a ainsi le pouvoir de réformer ou d'annuler la décision prise par l'autorité[2049].

À toutes ces procédures de droit commun s'ajoute également le référé-suspension[2050] ou le référé-liberté[2051] offrant une voie d'urgence pour contester les décisions prises par la CNIL. Le Conseil d'État embrasse donc un rôle historique central dans le contrôle du droit des données personnelles.

La variété de ces recours interroge sur la cohérence du droit des données à caractère personnel en résultant.

[2044] Pour le Conseil d'État, « les avis, recommandations, mises en garde et prises de position adoptés par les autorités de régulation dans l'exercice des missions dont elles sont investies, peuvent être déférés au juge de l'excès de pouvoir lorsqu'ils revêtent le caractère de dispositions générales et impératives ou lorsqu'ils énoncent des prescriptions individuelles dont ces autorités pourraient ultérieurement censurer la méconnaissance ou lorsqu'ils sont de nature à produire des effets notables, notamment de nature économique, ou ont pour objet d'influer de manière significative sur les comportements des personnes auxquelles ils s'adressent », CE Ass., 16 oct. 2019, *La Quadrature du Net et Caliopen*, n° 433069, *Lebon* p. 358, § 3.

[2045] CE Sec., 17 févr. 1950, *Ministre de l'agriculture* c. *Dame Lamotte*, n° 86949, *Lebon*. Selon Laferrière, « lorsque les actes et décisions de l'administration ont le caractère d'actes de commandement et de puissance publique, ils ne peuvent pas être révisés et réformés par la juridiction administrative ; ils ne peuvent être qu'annulés, et seulement pour illégalité, non pour inopportunité ou fausse appréciation des faits », É. Laferrière, *Traité de la juridiction administrative et des recours contentieux*, t. 1, 2e éd., Berger-Levrault, 1896, p. 15 s.

[2046] V. not. CE Sec., 28 mars 1997, *Solana*, n° 182912, *Lebon* p. 333 ; CE Sec., 5 déc. 2011, *Laffont*, n° 319545 et n° 338379, *Lebon* p. 609, v. P. Idoux, « L'existence d'un contrôle juridictionnel restreint du refus d'enquêter opposé par la CNIL », *AJDA* 2012, p. 959.

[2047] CE Sec., 3 oct. 2018, *M. de Lagausie*, n° 405939, *Lebon T.* p. 694. Pour une analyse de cette décision, v. not. T. Douville, « L'erreur de graphie d'un nom conduit le Conseil d'État à intensifier son contrôle des décisions de la CNIL », *Dalloz IP/IT* 2019, p. 115.

[2048] É. Laferrière, *Traité de la juridiction administrative et des recours contentieux*, t. 1, 2e éd., Berger-Levrault, 1896, p. 15 s.

[2049] *Rép. pén.* Dalloz, *Vo* « Autorités administratives indépendantes », par A. Cappello, 2016 (actu. 2019), nos 197 s.

[2050] Art. L. 521-1 du code de justice administrative.

[2051] Art. L. 521-2 du code de justice administrative.

B. Incohérence des recours

526. Les chevauchements de procédure. Toute loi, quelle que soit la qualité de sa rédaction, comporte toujours une part d'obscurité[2052]. Le droit des données personnelles n'échappe certainement pas à ce principe et, en dépit des nombreuses règles édictées, toutes les difficultés auxquelles les plaideurs sont exposés, ne sont pas résolues. L'une des particularités de cette matière est donc la variété d'acteurs spécialisés (tels que la CNIL, les autres autorités nationales de contrôle, le Comité Européen de la Protection des Données), et d'acteurs de droit commun (juges judiciaires et administratifs) qui sont sollicités pour interpréter ces textes. En réalité, c'est une véritable concomitance des procédures qui existe entre les autorités administratives indépendantes et les procédures ordinaires[2053]. Le législateur européen la tolère en ne prévoyant pas d'autorité de la chose décidée au bénéfice des autorités de contrôle et en n'aménageant aucune articulation entre les procédures[2054]. Quant à la loi française, seul l'article 22 de la loi Informatique et libertés anticipe la saisine simultanée de la CNIL et du juge ordinaire en prévoyant 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 ». Cette disposition évite ainsi une entorse à la règle *non bis in idem*[2055], laquelle veut qu'un même comportement ne puisse donner lieu à l'exercice de plusieurs poursuites ou au prononcé de plusieurs sanctions[2056]. Elle est conforme aux prescriptions établies par le Conseil constitutionnel affirmant que « une sanction administrative de nature pécuniaire ne peut se cumuler avec une sanction pénale »[2057]. En dehors de cette hypothèse, limitée à l'organisation de la sanction, le

---

[2052] L. Boré, « Les deux fonctions des juridictions suprêmes », *JCP G* 2018, nº 1-2, p. 33, § 4.
[2053] P. Gélard, « Rapport sur les autorités administratives indépendantes. Office parlementaire d'évaluation de la législation », Sénat, nº 404, 15 juin 2006, p. 115.
[2054] L'article 79 du règlement UE nº 2016/679 énonce que les réclamations devant les autorités de contrôle sont effectuées « sans préjudice de tout autre recours administratif ou extrajudiciaire », ce qui laisse présager que le législateur avait non seulement anticipé ce chevauchement de procédure mais qu'il l'avait accepté. Quant à l'article 81 de ce texte, il se limite aux seuls conflits de juridictions entre États membres.
[2055] F. Mattatia, *La protection des données à caractère personnel face aux usages illicites, déloyaux et frauduleux*, th. Paris X, 2010, p. 361.
[2056] Sur la différence entre les deux acceptions, v. par ex., D. Bernard, « Article 50 – Droit à ne pas être jugé ou puni pénalement deux fois pour une même infraction », in *Charte des droits fondamentaux de l'Union européenne. Commentaire article par article*, dir. F. Picod et S. Van Drooghenbroeck, nº 1, p. 1039 s. Plus largement sur la règle *non bis in idem*, v. J. Lelieur-Fischer, *La règle ne bis in idem : du principe de l'autorité de la chose jugée au principe d'unicité d'action répressive. Étude à la lumière des droits français, allemand et européen*, th. Paris I, 2005 ; F. Drummond, « Le fabuleux destin de la règle *non bis in idem* », *Bulletin Joly Bourse* 2014, nº 12, p. 605 ; J. Chacornac, « L'articulation des répressions. Comment résoudre le problème de *non bis in idem* ? », *RSC* 2019, p. 333.
[2057] Cons. const., 23 juill. 1996, nº 96-378 DC, cons. 15.

principe est que les procédures suivent leur cours devant les différentes instances sans que l'une d'elles ne soit contrainte de sursoir à statuer[2058]. Ainsi, le juge civil et la CNIL pourraient être sollicités simultanément[2059].

Un tel chevauchement de procédure est préjudiciable pour la cohérence d'ensemble résultant du droit des données à caractère personnel. À ces risques de chevauchement de procédures s'ajoutent également les problèmes liés aux conflits d'interprétation d'une même règle par les différentes juridictions.

527. Les chevauchements d'interprétation. L'article 6 de la Déclaration des droits de l'homme établit le principe d'égalité de tous devant la loi en affirmant que celle-ci doit être la même pour tous, soit qu'elle protège soit qu'elle punisse. Pour parvenir à cet objectif, il ne suffit pas d'assurer l'unité des textes, il faut également garantir l'unité de leur interprétation[2060]. En principe, ce rôle essentiel revient aux juridictions suprêmes chargées de produire, au fil de leurs décisions, une interprétation unifiée de la règle de droit[2061]. Au sommet de leurs ordres juridictionnels respectifs, le Conseil d'État et la Cour de cassation garantissent donc l'application cohérente des règles par les juridictions du fond. Ce rôle unificateur a été renforcé par la consécration de la procédure de renvoi pour avis instituée devant le Conseil d'État en 1987[2062] et de la procédure pour avis établie devant la Cour de cassation en 1991[2063].

Ce rôle est mis à mal en droit des données personnelles puisque les deux ordres de juridiction sont amenés à se prononcer sur l'interprétation des mêmes dispositions. Comme le remarquaient justement Madame Céline Wiener et Herbert Maisl,

---

[2058] Le Conseil d'État semble même considérer que la CNIL ne peut refuser d'instruire une plainte en se fondant sur le « seul motif qu'une juridiction avait à connaître de ces faits », v. CE Sec., 30 mai 2001, n° 219731, inédit *Lebon*.

[2059] Il convient toutefois de noter que le risque d'entorse à la règle *non bis in idem* serait moindre puisque le juge civil est, en droit positif, amené à réparer le préjudice causé par un manquement au droit des données à caractère personnel, alors que l'autorité de contrôle prononce des amendes administratives. Sur les difficultés soulevées par ce type de cumuls, v. N. Allix, *Les sanctions pécuniaires civiles,* th. Paris II, 2020, n^os^ 655 s., p. 529 s.

[2060] R. Perrot, B. Beignier et L. Miniato, *Institutions judiciaires*, 17^e^ éd., LGDJ, 2018, n° 219.

[2061] L. Boré, « Les deux fonctions des juridictions suprêmes », *JCP G* 2018, n° 1-2, p. 33, § 14 ; D. Foussard, « La Cour de cassation et l'unification du droit », in *Les cours judiciaires suprêmes dans le monde arabe*, colloque de Beyrouth, 13 et 14 mai 1999, Bruylant, 2001, p. 161 s.

[2062] Art. 12 de la loi n° 87-1127 du 31 déc. 1987 portant réforme du contentieux administratif, *JORF* 1 janv. 1988, n° 0001, p. 7 ; v. B. Martin-Laprade, « Le filtrage des pourvois et les "avis" contentieux », *AJDA* 1988, p. 85 ; D. Labetoulle, « Ni monstre, ni appendice : le "renvoi" de l'article 12 », *RFDA* 1988, p. 213.

[2063] Loi n° 91-491 du 15 mai 1991 modifiant le code de l'organisation judiciaire et instituant la saisine pour avis de la Cour de cassation, *JORF* 18 mai 1991, n° 0115, p. 6790. Pour une analyse de cette loi, v. A. Coeuret, « Loi n° 91-491 du 15 mai 1991 modifiant le code de l'organisation judiciaire et instituant la saisine pour avis de la Cour de cassation », *RTD civ.* 1991, p. 615 ; F. Zenati, « La saisine pour avis de la Cour de cassation », *D.* 1992, p. 247. En matière pénale, cette procédure pour avis n'a été instituée que suite à l'adoption de l'article 26 de la loi organique n° 2001-539 du 25 juin 2001 relative au statut des magistrats et au Conseil supérieur de la magistrature, *JORF* 26 juin 2001, n° 0146, texte 1.

« l'interprétation de la loi ne se réduit pas en une opération mécanique consistant à dégager le sens préexistant d'un texte ; il y a souvent création intellectuelle, apport nouveau de la part de l'interprète, surtout aujourd'hui avec la complexité que revêtent certaines législations. Ainsi le juge, avec l'autorité qui est la sienne, peut-il imposer sa propre représentation du sens des textes et de la manière dont ils doivent se combiner entre eux, alors même que d'autres interprétations seraient tout aussi concevables. Cette politique jurisprudentielle est inévitable »[2064]. S'il est admis que nul n'a de droit acquis à une jurisprudence figée[2065], il faut tout de même espérer que les divergences d'interprétation entre les deux ordres ne soient pas telles qu'une même règle de droit puisse être interprétée d'une certaine façon devant les juridictions administratives et d'une façon diamétralement opposée devant les juridictions judiciaires[2066]. L'antagonisme de ces solutions ne pourrait pas être résolu car les décisions contradictoires demeurent intactes, protégées chacune par leur ordre de juridiction[2067]. De telles divergences ont déjà existé dans l'interprétation du droit des données personnelles. Par exemple, pendant longtemps, le juge judiciaire n'avait pas reconnu aux adresses IP le statut de données personnelles, alors même que le Conseil d'État avait admis une telle qualification[2068]. Ainsi, selon que les parties sont attraites devant l'un ou l'autre ordre juridictionnel, elles peuvent être soumises à des interprétations

---

[2064] H. Maisl et C. Wiener, note ss CE Sec., 19 mai 1983, *D.* 1983, p. 546.

[2065] La Cour de cassation affirme que la sécurité juridique « ne saurait consacrer un droit acquis à une jurisprudence figée, l'évolution de la jurisprudence relevant de l'office du juge dans l'application du droit », v. Cass. civ. 1re, 21 mars 2000, nº 98-11.982, *Bull. civ.* 2000, I, nº 97, p. 65. Le Conseil d'État quant à lui considère que le requérant « ne pouvait se prévaloir d'un principe de sécurité juridique énoncé à l'article 6 de la Convention européenne des droits de l'homme pour soutenir que la légalité [d'un acte administratif] n'aurait dû être appréciée qu'au regard de la jurisprudence établie à la date où il a été prononcé », v. CE Sec., 14 juin 2004, *Société civile immobilière Saint-Lazare,* nº 238199, *Lebon T.* p. 692. Pour une étude liée à la rétroactivité de la jurisprudence, G. Drouot, *La rétroactivité de la jurisprudence. Recherche sur la lutte contre l'insécurité juridique*, th. Paris II, 2014, LGDJ.

[2066] Déjà en 1988, Monsieur Jean Frayssinet relevait de tels cas de différence d'interprétations entre le Conseil d'État et la Cour de cassation, et selon lui « une telle situation, qui ferait varier fortement la portée d'une même loi suivant l'ordre juridictionnel compétent, serait inadmissible pour le justiciable et sur le plan pratique, comporterait des risques de décisions contradictoires qui, dans certains cas de figure imaginables, relèveraient de la capacité de jugement au fond du tribunal des conflits », v. J. Frayssinet, « La Cour de cassation et la loi informatique, fichiers et libertés, ou comment amputer une loi tout en raffermissant son application », *JCP G* 1988, I, p. 3323.

[2067] P. Gélard, « Rapport sur les autorités administratives indépendantes. Office parlementaire d'évaluation de la législation », Sénat, nº 404, 15 juin 2006, p. 117. Une question préjudicielle pourra quand même être posée à la Cour de justice de l'Union européenne.

[2068] Dès 2007, le Conseil d'État avait validé l'idée selon laquelle une adresse IP est une donnée à caractère personnel, v. CE Sec., 23 mai 2007, *Sacem,* nº 288149, inédit *Lebon*, pour une analyse de l'arrêt v. not. S. Grégoire, « Le statut de l'adresse IP : conséquences sur les mécanismes de constat, d'avertissement et de sanction du *peer to peer* envisagés par les accords de l'Élysée et le projet de loi "Création et Internet" », *Légicom* 2009, nº 43, p. 103. Cette interprétation a été confirmée en 2014, v. CE Sec., 12 mars 2014, *Pages Jaunes Groupe*, nº 353193, *Lebon T.* p. 663. La Cour de cassation, dans un arrêt du 13 janvier 2009, avait affirmé que le fait de relever une adresse IP pour pouvoir localiser par le biais du fournisseur d'accès à Internet l'auteur des contrefaçons ne constituait pas un traitement de données à caractère personnel, refusant à demi-mot de qualifier les adresses IP comme des données à caractère personnel, v. Cass. crim., 13 janv. 2009, nº 08-84.088, *Bull. crim.* 2009, nº 13. Ce n'est qu'en 2016 que la Cour de cassation a rejoint l'interprétation selon laquelle l'adresse IP est une donnée à caractère personnel, v. Cass. civ. 1re, 3 nov. 2016, nº 15-22.595, *Bull. civ.* 2016, nº 206, p. 251.

différentes de la même règle de droit. L'insécurité juridique générée par ces différences d'interprétation est préjudiciable pour les responsables du traitement, ainsi que pour les personnes concernées. Les premiers se voient soumis à des obligations contradictoires alors que les seconds ne bénéficient pas des mêmes protections. Ces divergences entre les ordres de juridiction sont d'autant plus problématiques que le système juridique français ne comprend pas de mécanisme apte à les briser et à unifier l'interprétation de la règle de droit[2069].

La fragmentation des recours entame donc la mission régulatrice et unificatrice des plus hautes juridictions et génère un risque d'atteinte à la sécurité juridique et au principe d'égalité. Surtout, cette fragmentation renforce le sentiment que le droit des données personnelles est un droit complexe, réservé aux initiés. Un encadrement de ces recours paraît donc nécessaire.

§ II. Des recours à canaliser

528. Plan. Une mise en œuvre plus cohérente du droit des données personnelles passe par un renforcement du rôle du juge judiciaire dans ce contentieux (A) ainsi que par le renforcement des actions collectives (B).

A. Renforcer le rôle du juge judiciaire

529. L'autorité judiciaire, gardienne de la liberté individuelle. Ce n'est pas un hasard si l'article 66 de la Constitution a désigné l'autorité judiciaire comme la gardienne des libertés individuelles. Sa légitimité est justifiée par son indépendance constitutionnellement garantie[2070]. Cette indépendance est inhérente à la fonction du juge qui se doit d'être neutre par rapport au litige qui lui est présenté[2071]. Le droit français organise donc l'indépendance de l'autorité judiciaire à l'égard du gouvernement, du législateur et des parties[2072].

Le Conseil constitutionnel est longtemps resté fidèle à une interprétation étendue de l'article 66 de la Constitution et de la notion de liberté individuelle, en

---

[2069] P. Gélard, « Rapport sur les autorités administratives indépendantes. Office parlementaire d'évaluation de la législation », Sénat, nº 404, 15 juin 2006, p. 115.
[2070] Cette indépendance est organisée à l'article 64 de la Constitution, v. B. Louvel, « L'autorité judiciaire, gardienne de la liberté individuelle ou des libertés individuelles ? », Rencontre annuelle des premiers présidents de cour d'appel et de la Cour de cassation, 2 févr. 2016.
[2071] N. Cayrol, *Procédure civile*, Dalloz, 2e ed., 2019, nº 437, p. 200.
[2072] N. Cayrol, *Procédure civile*, Dalloz, 2e ed., 2019, nos 438 s., p. 200 s.

censurant les dispositions confiant au juge administratif le pouvoir de veiller à sa protection[2073]. Néanmoins, au milieu des années 1980, le Tribunal des conflits[2074] et le Conseil d'État[2075] ont retenu une interprétation plus circonscrite de l'article 66 de la Constitution. Ils ont été rejoints par le Conseil constitutionnel dans une série de décisions de 1999[2076]. Le Conseil constitutionnel a stabilisé sa jurisprudence autour d'une définition plus étroite de la liberté individuelle, en se référant à l'article 66 de la Constitution uniquement dans le domaine des privations de liberté (garde à vue, détention, rétention ou hospitalisation sans consentement)[2077]. La conséquence directe de cette interprétation a été de permettre au juge administratif d'intervenir dans la garantie des libertés, notamment celles liées à la protection des données personnelles[2078].

530. La place centrale du Conseil d'État dans le droit des données personnelles. L'une des spécificités du Conseil d'État est relative aux missions qu'il exerce : celle de conseiller le Gouvernement et celle de juger les litiges relatifs aux actes des administrations. Cette double compétence place le Conseil d'État en véritable boussole du droit des données à caractère personnel. En effet, il intervient à toutes les étapes de ce droit : dans la *conception* et les *modifications* législatives puisqu'il est consulté sur les projets de lois ou les ordonnances[2079] ; dans l'*application* de ces règles puisqu'il rend des avis à l'occasion de l'élaboration des normes réglementaires ; mais surtout

---

[2073] Plusieurs décisions du Conseil constitutionnel attestaient de son contrôle strict dès que la liberté individuelle est en jeu, v. not. Cons. const., 12 janv. 1977, nº 76-75 DC, cons. 5 ; Cons. const., 29 déc. 1983, nº 83-164 DC, cons. 28 s. et Cons. const., 13 août 1993, nº 93-325 DC, cons. 9. L'analyse de ces décisions confirme ce contrôle strict, v. P. Gaïa, R. Ghevontian, F. Mélin-Soucramanien, A. Roux et E. Oliva, *Les grandes décisions du Conseil constitutionnel*, 19e éd., Dalloz, 2018, nº 31, p. 474, § 6 ; nº 60, p. 968, § 12 ; nº 34, p. 534, § 7. Monsieur Floran Vadillo affirme que l'article 66 avait, dès le départ, une portée bien moindre que celle défendue par le Conseil constitutionnel puisque son application aurait été circonscrite à la question de la détention arbitraire, négatif de la liberté individuelle, v. F. Vadillo, « Liberté individuelle vs liberté personnelle : l'article 66 de la Constitution dans la jurisprudence du Conseil constitutionnel ou la progressive reconnaissance d'un habeas corpus à la française », *LPA* 22 avr. 2015, nº 80, p. 4.

[2074] Tribunal des conflits, 9 juin 1986, *Commissaire de la République de la région d'Alsace et autres,* nº 02434, *Lebon* p. 301.

[2075] CE Ass., 8 avr. 1987, *Ministère de l'intérieur et de la décentralisation,* nº 55895, *Lebon* p. 128.

[2076] Cons. const., 23 juill. 1999, nº 99-416 DC, cons. 45 ; Cons. const., 9 nov. 1999, nº 99-419 DC, cons. 73 ; Cons. const., 21 déc. 1999, nº 99-422 DC, cons. 52. Sur la liberté d'aller et venir, v. Cons. const., 16 juin 1999, nº 99-411 DC, cons. 20. Sur la liberté du mariage, v. Cons. const., 20 nov. 2003, nº 2003-484 DC, cons. 94.

[2077] Commentaire de la décision du Conseil constitutionnel, 29 nov. 2013, nº 2013-357 QPC, p. 7.

[2078] Comme le remarquent Messieurs François Terré et Nicolas Molfessis, « l'évolution se caractérise, sous l'effet de luttes d'influence et d'enjeux politiques, par une intrusion progressive du juge administratif dans le contrôle des atteintes aux libertés individuelles », v. F. Terré et N. Molfessis, *Introduction générale au droit*, 11e éd., Dalloz, 2019, nº 194, p. 221 s.

[2079] Art. 39 de la Constitution du 4 août 1958. Depuis la réforme constitutionnelle du 23 juillet 2008, le Conseil d'État peut également être consulté sur les propositions de lois.

dans la *réalisation* de ce droit puisqu'il est compétent pour connaître des recours contre les décisions de la CNIL[2080].

En plus de ses larges pouvoirs institutionnels, le Conseil d'État réussit à propager sa doctrine au-delà de ses murs, au travers des détachements de ses membres au sein des cabinets ministériels[2081], et grâce à son ample représentation dans le collège de la CNIL[2082].

Tous ces éléments font du Conseil d'État l'acteur central de la mise en œuvre du droit des données à caractère personnel. Une telle place requiert donc une application irréprochable des principes d'indépendance et d'impartialité. Ces principes sont d'autant plus essentiels qu'ils garantissent aux justiciables que l'acte de juger sera uniquement déterminé par les arguments du débat judiciaire, en dehors de toute pression et de tout préjugé.

531. L'effectivité relative des principes d'indépendance et d'impartialité. Contrairement à l'indépendance de l'autorité judiciaire, celle des juridictions administratives n'est pas prévue par la Constitution puisque les dispositions de l'article 64 de la Constitution ne leur sont pas applicables[2083]. L'indépendance de ces juridictions a toutefois été identifiée en 1980 par le Conseil constitutionnel comme un principe fondamental reconnu par les lois de la République[2084]. La loi du 20 avril 2016 relative à la déontologie a considérablement renforcé les obligations déontologiques prévues à l'égard des membres de la juridiction administrative, en affirmant notamment que les « membres du Conseil d'État exercent leurs fonctions en toute indépendance, dignité, impartialité, intégrité et probité et se comportent de façon à prévenir tout doute légitime à cet égard »[2085].

[2080] V. *supra*, nº 525.

[2081] Le Conseil d'État joue ainsi un rôle de réserve de personnel de haute qualité grâce aux dispositions très souples relatives au détachement qui permettent aux membres du Conseil, sans rompre le lien qui les unit à lui, de remplir pour un certain temps des fonctions dans l'administration, notamment dans les cabinets ministériels, v. J. Waline, *Droit administratif,* 28e éd., Dalloz, 2020, nº 645, p. 701.

[2082] Deux de ses membres y siègent et, depuis 1978, trois de ses huit présidents étaient des Conseillers d'État : Monsieur Michel Gentot a présidé l'institution pendant cinq ans (entre 1999 et 2004). Madame Isabelle Falque-Pierrotin a présidé la CNIL pendant près de huit années (entre 2011 et 2019) et Madame Marie-Laure Denis assure sa présidence depuis février 2019. Cette tendance à l'accaparation des postes à responsabilité au sein de la CNIL par les membres du Conseil d'État s'amplifie. En effet, depuis 2012 les trois secrétaires généraux qui se sont succédés à la tête des services de la CNIL étaient des maîtres des requêtes. Ainsi Monsieur Édouard Geffray a occupé le poste pendant cinq ans (entre 2012 et 2017), lui a succédé Monsieur Jean Lessi qui a occupé le poste pendant près de trois ans (2017 et 2020). Depuis le 11 avril 2020, c'est Monsieur Louis Dutheillet de Lamothe qui dirige les services de l'institution.

[2083] L. Favoreu *et al.*, *Droit constitutionnel,* 23e éd., Dalloz, 2020, nº 897, p. 693.

[2084] Cons. const., 22 juill. 1980, nº 80-119 DC, cons. 6

[2085] Article L. 131-2 du code de justice administrative modifié par la loi nº 2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires, *JORF* 21 avr. 2016, nº 0094, texte 2.

En pratique, l'effectivité de ces principes d'indépendance et d'impartialité ne peut-elle pas être questionnée, au moins à l'égard des parties ? En effet, la forte représentation des membres du Conseil d'État au sein du collège de la CNIL ne fait-elle pas planer des doutes sur l'impartialité de l'institution lorsque celle-ci statue sur les recours contre les décisions de la CNIL ? La théorie juridique des apparences[2086], développée par la jurisprudence de la CEDH, suppose que le principe d'impartialité ne serait pas respecté toutes les fois où le justiciable peut craindre que les membres de la juridiction ne soient pas parfaitement libres dans leur prise de décision[2087]. Selon cette théorie, « le simple doute suffit à altérer l'impartialité du tribunal en question »[2088]. Ce doute n'est-il pas caractérisé lorsque le Conseil d'État est amené à se prononcer sur des décisions prises par des collègues ? Ces doutes sont d'autant plus forts que, depuis bientôt dix ans, les présidentes successives de l'autorité étaient des conseillers d'État[2089]. Ces remarques quant à l'impartialité du Conseil d'État commandent de formuler certaines propositions.

532. Les arguments en faveur du renforcement de la compétence du juge judiciaire. Plusieurs arguments apparaissent favorables au renforcement de la compétence du juge judiciaire dans le contentieux du droit des données à caractère personnel. Tout d'abord, outre la reconnaissance constitutionnelle de sa fonction de gardien des libertés, le juge judiciaire est la sentinelle désignée pour veiller au respect des droits de la personnalité[2090]. En effet, il connaît du contentieux lié aux délits de presse, aux atteintes à la vie privée, et à la responsabilité extracontractuelle. Il est également le juge historique et constitutionnel en matière de protection de la liberté individuelle[2091]. Dès 1993, le Conseil constitutionnel reconnaissait que les dispositions prévues par la loi Informatique et libertés sont « protectrices de la liberté individuelle »[2092]. Si l'étendue de la notion de liberté individuelle a évolué, l'article 1er

---

[2086] A. Fittie-Duval, « La théorie des apparences, nouveau paradigme de l'action publique ? », *AJDA* 2018, p. 440.
[2087] La CEDH a introduit cette théorie en 1970 et l'a ensuite développée dans d'autres décisions, v. not. CEDH, 17 janv. 1970, *Delcourt* c. *Belgique,* nº 2689/65, § 31 ; CEDH, 30 oct. 1991, *Borgers* c. *Belgique*, nº 12005/86, § 24.
[2088] La CEDH s'est prononcée pour savoir si le Conseil d'État luxembourgeois, dont les membres cumulent deux fonctions (consultative et contentieuse), remplissait les exigences d'impartialité et a considéré que « le seul fait que certaines personnes exercent successivement, à propos des mêmes décisions, les deux types de fonctions est de nature à mettre en cause l'impartialité structurelle de ladite institution », v. CEDH, 28 sept. 1995, *Procola* c. *Luxembourg,* nº 17570/89, § 45.
[2089] V. *supra*, nº 530.
[2090] G. Loiseau, « Droits de la personnalité. Janv. 2011 – déc. 2011 », *Légipresse* 2012, nº 290, p. 60.
[2091] V. *supra*, nº 529.
[2092] Cons. const., 20 janv. 1993, nº 92-316 DC, cons. 14. En matière de vidéosurveillance, le Conseil constitutionnel avait également affirmé que « compte tenu des risques que peut comporter pour la liberté

de cette loi proclame toujours que l'informatique ne doit pas porter atteinte aux libertés individuelles et reconnaît le rôle de ce droit dans leur protection. Par ailleurs, et comme le remarque Madame Agathe Lepage, la loi du 6 janvier 1978 reconnaît « plusieurs droits à la personne dont les données à caractère personnel sont concernées par un traitement, (…) dans lesquels on voit des droits de la personnalité »[2093]. Le droit des données à caractère personnel concerne donc bel et bien les droits de la personnalité et, dans une certaine mesure, la liberté individuelle ; domaines qui relèvent de la compétence naturelle du juge judiciaire. Afin de rendre la mise en œuvre de cette matière plus effective, le juge judiciaire devrait y trouver un rôle plus important, particulièrement pour les recours contre les décisions de la CNIL.

À l'instar de ce qui a été prévu pour d'autres autorités administratives indépendantes[2094], le contentieux lié à ces actes pourrait être réparti en fonction du type de pouvoir exercé. L'exercice du pouvoir réglementaire, dont le caractère administratif n'est pas contestable, pourrait relever du Conseil d'État[2095] ; quant au pouvoir de règlement des différends, notamment ceux liés aux décisions de sanction prises sur le fondement des articles 58 et 78 du règlement européen, celui-ci pourrait relever de la cour d'appel de Paris[2096]. Le renforcement de la place du juge judiciaire dans les recours en matière de données personnelles présente donc plusieurs avantages et s'inscrit dans la tradition juridique française.

B. Encourager les actions collectives

533. La protection des données personnelles comme valeur commune. Longtemps présenté comme un bouclier fourni à l'individu pour se défendre contre les traitements illicites de ses données, le droit des données personnelles évolue afin de devenir une

individuelle l'installation de systèmes de vidéosurveillance, il ne peut subordonner à la diligence de l'autorité administrative l'autorisation d'installer de tels systèmes sans priver alors de garanties légales les principes constitutionnels », v. Cons. const., 18 janv. 1995, nº 94-352 DC, cons. 12.

[2093] *Rép. civ.* Dalloz, *Vº* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), nº 31.

[2094] H. Lécuyer, « Les autorités administratives indépendantes et le dualisme juridictionnel », *Revue de droit d'Assas* 2019, nº 18, p. 71 s. D'ailleurs, comme le remarquait le Conseil constitutionnel dans une décision relative au Conseil de la concurrence, « lorsque l'application d'une législation ou d'une réglementation spécifique pourrait engendrer des contestations contentieuses diverses qui se répartiraient, selon les règles habituelles de compétence, entre la juridiction administrative et la juridiction judiciaire, il est loisible au législateur, dans l'intérêt d'une bonne administration de la justice, d'unifier les règles de compétence juridictionnelle au sein de l'ordre juridictionnel principalement intéressé », v. Cons. const., 23 janv. 1987, nº 86-224 DC, cons. 16.

[2095] *Rép. cont. adm.* Dalloz, *Vº* « Autorités de régulation », par E. Guillaume et L. Coudray, 2010 (actu. 2016), nºs 32 s.

[2096] C'est devant cette cour que les recours contre les décisions du Autorité de la concurrence sont formés, v. *Rép. cont. adm.* Dalloz, *Vº* « Autorités de régulation », par E. Guillaume et L. Coudray, 2010 (actu. 2016), nºs 32 s. ; v. aussi P. Gélard, « Rapport sur les autorités administratives indépendantes. Office parlementaire d'évaluation de la législation », Sénat, nº 404, 15 juin 2006, p. 117.

véritable forteresse pour la société dans son ensemble. En effet, avec le numérique, la protection des données et de la vie privée « n'est plus seulement perçue comme une valeur individuelle donnant lieu à une micro-protection à l'échelle de la personne s'estimant victime d'un trouble ; elle se présente comme une valeur sociale qui nécessite une macro-défense pour assurer, au-delà des intérêts particuliers, la préservation de l'intérêt social qui s'attache à sa garantie collective »[2097]. En reconnaissant aux individus la possibilité d'agir collectivement contre les traitements illicites, le législateur a implicitement affirmé le caractère récurrent, chronique et répandu de ces atteintes[2098]. Les groupements[2099], grâce aux actions collectives, favorisent la reconnaissance d'une valeur sociale à la protection des données personnelles, notamment parce que ces actions témoignent des problèmes systémiques engendrés par les manquements au droit des données à caractère personnel.

Par ailleurs, ces actions juridictionnelles permettent de contourner l'immobilisme des « autorités chef de file » et l'inertie des autorités de contrôle asphyxiées par les nombreuses plaintes dont elles sont saisies[2100]. En effet, l'article 79 du règlement européen reconnaît la compétence du juge français pour les affaires impliquant des victimes ayant leur résidence habituelle en France.

Pourtant, des limites procédurales restreignent encore trop largement ces actions collectives, les empêchant ainsi de prendre toute la place qu'elles devraient avoir.

534. L'encadrement strict de l'intérêt à agir pour les recours collectifs. La question de la qualité à agir pour porter des recours collectifs a cristallisé de nombreux débats. Le dispositif actuel restreint délibérément les titulaires de ces recours, particulièrement pour l'action de groupe[2101]. Si l'avocat est souvent celui qui initie la

---

[2097] G. Loiseau, « Droits de la personnalité. Janv. 2011 – déc. 2011 », *Légipresse* 2012, n° 290, p. 60 ; J. Fraifield et C. Engel, « Privacy as a public good », *Duke Law Journal* 2015, vol. 65, p. 385 s. [65 DUKE L.J. 385], spéc. p. 421 s.

[2098] D'ailleurs, selon Madame Sandie Alliot, la donnée personnelle devrait être qualifiée comme un bien commun, lequel est caractérisé par « la volonté des personnes d'agir ensemble pour assurer la pérennité de ces biens », v. S. Alliot, *Essai de qualification de la notion de données à caractère personnel,* th. Besançon, 2018, n[os] 511 s., p. 231 s. Plus largement, Madame Nathalie Martial-Braz s'interrogeait récemment sur l'opportunité d'intégrer « un droit fondamental du numérique tenant à la préservation du caractère commun de la donnée et plus largement de l'Internet dans l'environnement numérique », N. Martial-Braz, « La transdisciplinarité du droit du numérique », in *Mélanges M. Vivant*, 2020, Dalloz, p. 849 s., n° 16, spéc. p. 860.

[2099] Pour une étude de cette notion, v. F. Sarda, « Rapport français », in *Travaux de l'Association Henri Capitant*, « Les groupements », t. 45, Journées japonaises, Litec, 1994, p. 49 s., spéc. p. 53 s.

[2100] V. *supra,* n° 508.

[2101] Cet encadrement était déjà présent dans le rapport dirigé par Monsieur Jean Calais-Auloy de 1985 qui affirmait que « aux États-Unis et au Québec, l'action peut être intentée par n'importe quel membre du groupe. Ce système n'est pas satisfaisant, car on peut craindre que le demandeur ne soit manipulé par des tiers dont les intérêts ne coïncident pas nécessairement avec ceux des consommateurs. La Commission préfère donc réserver l'action de groupe aux organisations représentatives de consommateurs », v. J. Calais-Auloy (dir.), « Propositions pour un

class action aux États-Unis, le législateur français, hanté par la peur que les avocats ne favorisent leur rémunération avant celle des victimes[2102], ne leur a pas reconnu ce pouvoir[2103]. Seuls certains groupements limitativement énumérés peuvent intenter ces actions. Ainsi, l'article 37 de la loi Informatique et libertés reconnaît la qualité à agir aux « associations régulièrement déclarées depuis *cinq ans* au moins ayant dans leur objet statutaire la protection de la vie privée ou la protection des données à caractère personnel », aux « associations de défense des consommateurs représentatives au niveau national et agréées » ainsi qu'aux organisations syndicales représentatives[2104]. Plusieurs raisons ont encouragé le législateur à encadrer si strictement l'intérêt à agir des groupements[2105].

535. Justifications de l'encadrement strict de l'intérêt à agir. Le législateur français a voulu éviter à tout prix de reproduire les dérives du modèle américain de la *class action*[2106]. En effet, de nombreux auteurs redoutaient l'instrumentalisation de l'accès à la justice[2107], les abus[2108], ou encore le dévoiement de l'action pour servir des

---

nouveau droit de la consommation, Rapport de la commission de refonte du droit de la consommation au secrétaire d'État auprès du ministre de l'Économie, des Finances et du Budget chargé du Budget et de la Consommation », La Documentation Française, 1985, p. 131.

[2102] D. Mainguy, « Introduction en droit français des *class actions* », *LPA* 22 déc. 2005, nº 254, p. 6, § 76 s. ; R. Hammadi et A. Le Lock, « Rapport sur le projet de loi relatif à la consommation », Assemblée nationale, nº 1156, 13 juin 2013, p. 40 et p. 55 ; P. Montfort, « Action de groupe à la française : garantir l'accès au juge », *Gaz. Pal.* 2013, nº 136, p. 27.

[2103] En France, l'on considère souvent que « l'avocat doit préserver une distance par rapport à son client. "Incarner" un client et figurer sur le devant de la "scène judiciaire" est de nature à supprimer cette distance. Tout schéma procédural dans lequel l'avocat se confond *de facto* avec son client est à proscrire », J.-D. Bretzner, « Ombres et lumières autour de la "qualité pour agir" dans l'action de groupe », *Gaz. Pal.* 2013, nº 136, p. 31. Pour une critique de cette place effacée de l'avocat, v. B. Vatier, « Peut mieux faire ! », *Gaz. Pal.* 2013, nº 136, p. 53. Les auteurs s'accordent tout de même pour relever le rôle central de l'avocat dans l'action de groupe, notamment dans la représentation des associations devant les juridictions. D'ailleurs, la représentation par avocat est obligatoire dès le tribunal de première instance, v. M. Bacache-Gibelli, *La responsabilité civile extracontractuelle,* 3e éd., Economica, 2016, nº 413, p. 484 ; v. aussi M. Bacache, « Action de groupe et responsabilité civile », *RTD civ.* 2014, p. 450 ; A. Guégan-Lécuyer, « La qualité pour agir exclusivement réservée à certaines associations », *Gaz. Pal.* 2013, nº 136, p. 23.

[2104] Déjà en 1996, Madame Marie-Anne Frison-Roche expliquait que « l'association est un groupement socialement légitime, car elle exprime un intérêt collectif objectif […]. Il faut admettre la *class action*, c'est-à-dire la voie par laquelle l'association vient défendre devant le juge un intérêt collectif spécifique », v. M.-A. Frison-Roche, « Le pouvoir processuel des associations et la perspective de la *class action* », *LPA* 24 avr. 1996, nº 50, p. 28.

[2105] Pour une étude sur les groupements, v. L. Boré, *La défense des intérêts collectifs par les associations devant les autorités administratives et judiciaires*, th. Paris I, 1997, LGDJ.

[2106] Pour une analyse des *class action* dans plusieurs systèmes juridiques, v. D. Mainguy, « Introduction en droit français des *class actions* », *LPA* 22 déc. 2005, nº 254, p. 6, § 6 s. Sur les limites mises en place par le législateur français pour prévenir les dérives de la *class action* américaine, v. C. de Perthuis, « L'action collective à la française : étude de droit comparé entre le droit français et le droit américain », *LPA* 25 mars 2014, nº 60, p. 21.

[2107] L'accès à la justice devenant alors une véritable technique de chantage, v. M.-A. Frison-Roche, « Le pouvoir processuel des associations et la perspective de la *class action* », *LPA* 24 avr. 1996, nº 50, p. 28.

[2108] V. Orif, « L'élaboration dans la loi J21 d'un modèle général d'action de groupe : un essai à transformer », *Gaz. Pal.* 2017, nº 285, p. 80.

intérêts extérieurs à ceux des victimes[2109]. Selon une opinion doctrinale, la restriction de la qualité à agir se justifie aisément : « il faut que le représentant soit digne de la tâche qu'il souhaite assumer, soit capable de l'assumer, il faut donc qu'il ait des intérêts identiques ou similaires aux membres du groupe »[2110]. Certains auteurs ont même été jusqu'à affirmer que cet encadrement protégeait les groupements prenant le risque de voir leur responsabilité engagée pour dénigrement si la responsabilité de l'auteur du préjudice de masse n'était pas reconnue[2111].

Il est évident que les conditions restrictives de l'intérêt à agir représentent un filtre à l'action de groupe et à l'effectivité de la défense des données personnelles[2112]. Cet encadrement illustre surtout une procédure principalement administrative et une forme un peu désuète de protection des personnes. En effet, de nouveaux types de regroupements informels se développent dans d'autres matières, notamment grâce aux outils numériques rendant plus aisée la mobilisation des personnes[2113].

Par ailleurs, dès l'instant où le législateur établit une liste de conditions pour ces groupements, le risque est de ne pas couvrir l'ensemble des situations dans lesquelles les actions collectives se justifient[2114]. Par exemple, l'association *None of Your Business,* instituée en 2017 par Monsieur Maximilian Schrems, pourtant très active dans le domaine de la protection des données personnelles, ne peut pas introduire d'action de groupe en France car elle n'a pas encore cinq années d'existence. Cet exemple est une illustration des problèmes liés à l'encadrement actuel de l'intérêt à agir.

536. Ouvrir à toute personne la possibilité d'introduire une action de groupe. Les premières formes de recours collectifs ont été introduites en droit français dans les années 1990[2115]. Depuis, quelques dizaines d'actions ont été introduites et peu d'entre

[2109] R. Hammadi et A. Le Lock, « Rapport sur le projet de loi relatif à la consommation », Assemblée nationale, nº 1156, 13 juin 2013, p. 40 et p. 55.
[2110] L. Boré, « Discours à la table ronde "Pour mieux réparer les préjudices collectifs : une *class action* à la française ?" », *Gaz. Pal.* 2001, nº 271, p. 4 ; dans le même sens, v. G. Wiederkehr, « La légitimité de l'intérêt pour agir », in *Mélanges S. Guinchard*, 2010, Dalloz, p. 877 s.
[2111] S. Guinchard, « Une *class action* à la française ? », *D.* 2005, p. 2180. Sur le risque de perdre le procès et l'atteinte à l'image pour l'association, v. M. J. Azar-Baud, « (In)action de groupe », *Gaz. Pal.* 2016, nº 23, p. 52.
[2112] A. Guégan-Lécuyer, « La qualité pour agir exclusivement réservée à certaines associations », *Gaz. Pal.* 2013, nº 136, p. 23.
[2113] Au sujet des actions de groupe en droit de la consommation, v. F. G'sell, « L'action des associations de consommateurs : à la recherche du groupe perdu », *Gaz. Pal.* 2014, nº 284, p. 15.
[2114] P. Montfort, « Action de groupe à la française : garantir l'accès au juge », *Gaz. Pal.* 2013, nº 136, p. 27.
[2115] Loi nº 92-60 du 18 janvier 1992 renforçant la protection des consommateurs.

elles ont abouti[2116]. Cet échec s'explique par les conditions très strictes de leur mise en œuvre, et notamment par le fait que seul un nombre très circonscrit d'associations pouvaient les intenter[2117]. Un sort similaire risque d'être réservé aux actions de groupe en droit des données personnelles en l'absence de modification législative. D'ailleurs, depuis l'entrée en application de la loi de juin 2018, une seule et unique action de groupe a été intentée en France[2118]. Pour prévenir un tel échec en droit des données personnelles, plusieurs propositions peuvent être formulées. La proposition la plus radicale est d'ouvrir l'exercice de l'action de groupe à toute personne[2119]. Certains auteurs plaident pour une solution plus modérée ouvrant la « porte de l'action de groupe à une association *ad hoc,* constituée après la réalisation des premiers préjudices, et dont le juge contrôlerait les gages de sérieux et de représentativité, voire de capacités matérielles et financières aux fins de délivrance d'un agrément judiciaire »[2120].

Dans tous les cas, la suppression de la condition relative aux cinq années d'existence est une nécessité[2121]. Elle est d'autant plus justifiée que les autres conditions de cette action sont encadrées strictement[2122].

Une fois la forme de recours décidée, l'une des difficultés auxquelles les personnes concernées doivent faire face est celle liée au régime de l'action.

SECTION II – FACILITER LES ACTIONS EN RESPONSABILITÉ

537. Les fonctions de la responsabilité. Classiquement, la réparation des préjudices passe par les mécanismes de responsabilité civile ou administrative. En droit civil, la responsabilité est classiquement définie comme toute obligation de répondre civilement

---

[2116] En droit de la consommation et dans le domaine de la santé, seule une petite dizaine d'actions de groupe auraient été intentées, M. J. Azar-Baud, « (In)action de groupe », *Gaz. Pal.* 2016, nº 23, p. 52. Un rapport parlementaire de 2020 a évalué à 21 le nombre total d'actions de groupe intentées depuis 2014 et regrette qu'aucune entreprise n'ait vu sa responsabilité engagée, v. L. Vichnievsky et P. Gosselin, « Rapport d'information sur le bilan et les perspectives des actions de groupe », Assemblée nationale, 11 juin 2020, nº 3085, p. 8.

[2117] L. Boré, « Le projet d'action de groupe : action mort-née ou premier pas ? », *Gaz. Pal.* 2013, nº 136, p. 29.

[2118] UFC-Que Choisir, « Action de groupe contre Google », 26 juin 2019. En novembre 2018, le groupement Internet Society France a mis en demeure la société Facebook. Les suites de cette mise en demeure n'ont pas été publiées, et il semble que la procédure judiciaire n'ait pas encore été engagée, v. Internet Society France, « L'Internet Society France, à travers son initiative E-Bastille, lance la première action de groupe contre Facebook et lui réclame 100 millions d'euros », 9 nov. 2018.

[2119] D. Mainguy, « Introduction en droit français des *class actions* », *LPA* 22 déc. 2005, nº 254, p. 6, § 94 s.

[2120] A. Guégan-Lécuyer, « La qualité pour agir exclusivement réservée à certaines associations », *Gaz. Pal.* 2013, nº 136, p. 23.

[2121] L'une des recommandations du récent rapport parlementaire appelle également à étendre le champ des associations ayant qualité à agir, L. Vichnievsky et P. Gosselin, « Rapport d'information sur le bilan et les perspectives des actions de groupe », Assemblée nationale, nº 3085, 11 juin 2020, p. 43 s.

[2122] Par exemple, le groupement est tenu d'ouvrir un compte à la Caisse des dépôts afin d'y déposer toute somme reçue au titre de l'indemnisation des consommateurs lésés, v. art. 623-10 du code de la consommation. Sur ce point, v. *Rép. proc. civ.* Dalloz, *Vº* « Action de groupe », par S. Ben Hadj Yahia, 2015 (actu 2019), nºs 83 s.

du dommage que l'on a causé à autrui[2123]. C'est pourquoi « on parle de responsabilité civile toutes les fois où une personne est tenue de réparer un préjudice subi par une autre et dans la genèse duquel elle se trouve impliquée »[2124]. Selon la belle expression du doyen Carbonnier, l'idée de la responsabilité civile vise à « faire en sorte que le dommage n'ait été qu'un rêve »[2125]. L'un des principaux buts de la responsabilité civile réside donc dans la réparation des dommages[2126]. Cette fonction indemnitaire s'allie traditionnellement à deux autres fonctions : celle de prévention, dont l'objectif est de dissuader les comportements antisociaux[2127], et celle de punition, qui vise à punir l'auteur pour ses actes illicites[2128]. La responsabilité ambitionne donc non seulement de sanctionner les comportements fautifs, mais aussi de prévenir le dommage en dissuadant l'auteur potentiel de le causer[2129]. Une mise en œuvre efficace des mécanismes de responsabilité contribue donc, en théorie au moins, à garantir indirectement le respect du droit des données personnelles.

538. La distinction entre la responsabilité contractuelle et la responsabilité extracontractuelle. Il est courant de distinguer la responsabilité contractuelle de la responsabilité extracontractuelle[2130]. La première est liée à l'existence d'un dommage causé dans le cadre d'un contrat alors que la seconde est liée à l'existence d'un dommage en rapport avec un fait dommageable[2131]. En droit des données à caractère personnel, ces deux types de responsabilité coexistent puisque, comme le remarque Monsieur Emmanuel Netter, le comportement blâmable d'un organisme traitant des données à caractère personnel peut constituer une violation des règles imposées par le droit des données à caractère personnel et, dans certains cas, il peut également

---

[2123] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vo* « Responsabilité », sens I.
[2124] N. Dejean de la Bâtie, *Droit civil français*, t. VI-2, dir. C. Aubry et C. Rau, 8e éd., Litec, 1989, no 1, p. 1.
[2125] J. Carbonnier, *Droit civil,* t. 4, *Les obligations*, 22e éd., PUF, 2000, no 198, p. 361.
[2126] P. Brun, *Responsabilité civile extracontractuelle*, 5e éd., LexisNexis, 2018, no 596, p. 411 ; rappr. G. Viney, P. Jourdain et S. Carval, *Les effets de la responsabilité,* 4e éd., LGDJ, 2017, no 116, p.153.
[2127] A. Tunc, « Responsabilité civile et dissuasion des comportements antisociaux », in *Mélanges M. Ancel*, t. 1, Pédone, 1975, p. 407 s., no 2, spéc. p. 407.
[2128] J. Rochfeld, *Les grandes notions du droit privé*, 2e éd., PUF, 2013, *Vo* « La responsabilité », no 6, p. 489. Sur les fonctions de la responsabilité civile délictuelle et une comparaison avec les fonctions de la responsabilité pénale, v. C. Dubois, *Responsabilité civile et responsabilité pénale. À la recherche d'une cohérence perdue,* th. Paris II, 2014, LGDJ, nos 13 s., p. 20 s.
[2129] P. Le Tourneau, « Des mérites et des vertus de la responsabilité civile », *Gaz. Pal.* 1985, no 1, p. 283, spéc. p. 284 s.
[2130] F. Chénédé, « Responsabilité contractuelle et responsabilité extracontractuelle : une *summa divisio* ? », in *Vers une réforme de la responsabilité civile française*, dir. B. Mallet-Bricourt, Dalloz, 2018, p. 31.
[2131] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vo* « Responsabilité », sens I.

constituer la violation d'un contrat passé avec la personne concernée[2132]. Comme l'écrivait Jean Carbonnier, « lorsque le droit positif met deux moyens juridiques à la disposition du même individu, le sens le plus élémentaire de ce double don est le cumul »[2133]. Si, dans de nombreuses situations, le plaideur peut choisir entre les différents fondements applicables, il n'en va pas toujours ainsi. En matière de responsabilité civile délictuelle par exemple, l'interaction entre les fondements aboutit à un blocage : c'est le cas de la responsabilité extracontractuelle qui est exclue lorsque les conditions d'application de la responsabilité contractuelle sont réunies[2134].

En droit des données à caractère personnel, c'est surtout la responsabilité extracontractuelle qui nous intéressera. Cela s'explique par le fait que c'est celle qui s'applique le plus souvent puisque c'est celle à laquelle renvoie le règlement européen et que son application pratique pose plusieurs difficultés.

539. Plan. Les conditions de la responsabilité en droit des données à caractère personnel entraînent des difficultés pratiques pour les victimes (§ I). Pour encourager les recours et garantir une meilleure protection des personnes, la mise en œuvre de la réparation doit donc être simplifiée (§ II).

§ I. *De lege lata* : les difficultés pour engager la responsabilité

540. La responsabilité dans le règlement européen. Le principe veut que toute personne qui a souffert d'un dommage du fait d'un manquement aux obligations résultant du droit des données personnelles puisse en demander réparation. Encore faut-il que la victime apporte la preuve des conditions propres à la réparation des atteintes aux données à caractère personnel. Celles-ci sont établies par l'article 82 du règlement européen, lequel prévoit dans son premier paragraphe que :

[2132] E. Netter, « L'extinction du contrat et le sort des données personnelles », *AJ Contrat* 2019, p. 416. V aussi sur l'articulation entre les deux régimes, A. Danis-Fatôme, « Quelles actions judiciaires en cas de violation du RGPD ? », *CCE* 2018, nº 4, dossier 18, § 8.
[2133] J. Carbonnier, ss. Cass. civ. 1re, 19 juill. 1960, *RTD civ.* 1961 p. 333.
[2134] Sur le cumul d'action, F. Bussy-Dunan, *Le concours d'action en justice entre les mêmes parties. L'étendue de la faculté de choix du plaideur,* 1987, th. Paris I, LGDJ. Pour une illustration récente de ce cumul, N. Balat, « Le cumul d'actions en droit des obligations », *D.* 2020, p. 1819.

> « 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 ».

Ces conditions de responsabilité font écho à celles de la responsabilité civile extracontractuelle française, c'est-à-dire le dommage, la faute et le lien de causalité[2135].

541. Plan. En l'absence de définition spéciale pour chacune des conditions prévues par l'article 82 du règlement européen, les juges français vont sans doute se référer aux définitions établies par le droit de la responsabilité civile délictuelle. En ce qui concerne le lien de causalité, c'est-à-dire la question de savoir si le fait dommageable a été la cause du dommage[2136], les principes du droit civil se transposent sans peine au droit des données à caractère personnel. En revanche, des difficultés apparaissent lors de la caractérisation de la faute (A) et du préjudice (B).

A. La faute

542. Plan. L'étude de la définition de la faute (1) précédera l'analyse des difficultés liées à sa preuve (2).

1. La définition de la faute

543. La faute civile. La notion de faute n'a nullement été définie par le code civil[2137]. Elle revêt des acceptions très variées et est d'autant plus délicate à saisir qu'elle est omniprésente[2138]. Pour pallier le silence du législateur, la doctrine a formulé d'innombrables propositions de définition[2139]. Entendue évasivement, la faute a été envisagée comme une « défaillance » ou une « erreur de conduite »[2140]. D'une manière

---

[2135] Pour une étude des difficultés relatives à l'action en responsabilité issue du règlement européen, L. Marignol, « Principe de responsabilité et action en responsabilité dans le Règlement général sur la protection des données (I) », *RLDI* 2020, n° 166, p. 44 ; « Principe de responsabilité et action en responsabilité dans le Règlement général sur la protection des données (II) », *RLDI* 2020, n° 167, p. 54.
[2136] F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, n° 1089, p. 1161.
[2137] M. Bacache-Gibelli, *La responsabilité civile extracontractuelle,* 3e éd., Economica, 2016, n° 143, p. 161 s. Pour une étude de la notion de faute, notamment en droit civil, v. A. Rabut, *De la notion de faute en droit privé,* th. Paris, 1946, LGDJ.
[2138] Sur le caractère ubiquitaire de la faute, v. G. Rouhette, « D'une faute, l'autre », *Droits* 1987, n° 5, p. 9. Sur les différentes fonctions de la responsabilité pour faute, v. J. Rochfeld, *Les grandes notions du droit privé*, 2e éd., PUF, 2013, *V°* « La responsabilité », n° 6, p. 488.
[2139] V. not. A. Rabut, *De la notion de faute en droit privé,* th. Paris, 1946, LGDJ.
[2140] V. par ex., J. Flour, J.-L. Aubert et E. Savaux, *Droit civil. Les obligations,* t. 2, *Le fait juridique,* 14e éd., Sirey, 2011, n° 98, p. 118.

plus restrictive, Planiol la définissait comme « le manquement à une obligation préexistante »[2141]. Bien que cette dernière définition ait ouvert une vive controverse doctrinale[2142], elle s'applique relativement bien au droit des données à caractère personnel.

544. La faute en droit des données à caractère personnel. Le droit des données à caractère personnel édicte, dans de pointilleux détails[2143], les obligations à la charge des organismes traitant des données. En conséquence, l'article 82 du règlement européen précise que la responsabilité de l'organisme responsable peut être engagée « du fait d'une violation du présent règlement ». Ainsi, en matière de données personnelles, c'est l'hypothèse la plus élémentaire de la faute délictuelle qui s'applique, c'est-à-dire celle résultant de la méconnaissance d'une norme de comportement imposée par une règle de droit écrit[2144]. La transgression de la norme est *en elle-même* constitutive d'une faute, de sorte que le pouvoir d'appréciation des juges est considérablement réduit[2145]. En effet, plus le texte est précis et les obligations déterminées, plus un caractère d'automaticité s'attache au constat de la faute[2146]. Ainsi, lorsque le juge constate une violation aux règles édictées par le droit des données personnelles, la faute sera caractérisée[2147]. Pour autant, toutes les atteintes causées par les traitements de données n'ouvrent pas toujours un droit à réparation.

545. Toutes les atteintes n'ouvrent pas un droit à réparation. Toutes les atteintes aux données à caractère personnel (telles que les accès non autorisés ou les détournements de données) ne permettent pas d'engager la responsabilité de l'organisme. L'exigence d'un manquement aux obligations prévues par le droit des données à caractère personnel est une condition nécessaire pour engager cette

---

[2141] M. Planiol, *Traité élémentaire de droit civil*, t. 2, 11e éd., LGDJ, 1931, no 863, p. 302 ; rappr. M. Bacache-Gibelli, *La responsabilité civile extracontractuelle,* 3e éd., Economica, 2016, no 143, p. 161.
[2142] V. not., H. et L. Mazeaud et A. Tunc, *Traité théorique et pratique de la responsabilité civile délictuelle et contractuelle,* t. 1, 6e éd., Montchrestien, 1965, no 392, p. 471 s. ; J. Flour, J.-L. Aubert et E. Savaux, *Droit civil. Les obligations,* t. 2, *Le fait juridique,* 14e éd., Sirey, 2011, no 98, p. 118.
[2143] Ces détails laissent tout de même d'importantes zones d'incertitude, v. N. Martial-Braz et J. Rochfeld (dir.), *Droit des données personnelles. Les spécificités du droit français au regard du RGPD*, Dalloz, 2019, nos 106 s., p. 17 s.
[2144] S. Porchy-Simon, *Droit civil 2e année. Les obligations,* 10e éd., Dalloz, 2017, no 736, p. 360.
[2145] P. Brun, *Responsabilité civile extracontractuelle*, 5e éd., LexisNexis, 2018, no 325, p. 220. Toutefois, les textes donnent souvent lieu à interprétation, en sorte que l'existence de la faute peut être discutée, v. not. la série d'arrêts rendus par la Cour de cassation au sujet du tabagisme passif, Cass. civ. 2e, 13 juin 2013, no 12-22.170, *Bull. civ.* 2013, II, no 124.
[2146] *Rép. civ.* Dalloz, *Vo* « Responsabilité du fait personnel », par P. Brun, 2015 (actu. 2020), no 89.
[2147] Pour une critique de cette automaticité, v. M. Dugué, « La définition de la faute civile », *RDC* 2019, no 116, p. 175.

responsabilité. Ainsi, par exemple, toutes les violations de données personnelles[2148] n'ouvrent pas un droit à réparation aux victimes. En effet, si l'organisme démontre la mise en œuvre de l'ensemble des mesures nécessaires pour prévenir une telle violation et fournit la preuve du respect de ses obligations de notification, la faute ne sera pas caractérisée, et sa responsabilité ne pourra pas être engagée. Ce principe rappelé, il convient désormais de montrer les difficultés entourant la démonstration de la faute.

2. La preuve de la faute

546. Charge de la preuve. En application du principe *actori incombit probatio*, la victime doit apporter la preuve de la faute, c'est-à-dire démontrer le manquement au droit des données personnelles[2149]. Les modes de preuve de la faute civile sont ceux des faits juridiques : elle peut donc être établie par tous moyens[2150], et le principe selon lequel nul ne peut se constituer de preuve à soi-même ne lui est pas applicable[2151]. En apparence, le système de preuve est donc favorable aux victimes puisque celles-ci bénéficient d'un champ immense d'éléments pour démontrer la violation. Pourtant, en pratique, cette preuve s'avère souvent délicate à apporter pour les victimes.

547. La variété des obligations prévues par le droit des données personnelles. La diversité des obligations prévues par le règlement européen emporte une grande variété des violations possibles. La preuve de certaines d'entre elles peut être relativement facile à apporter (par exemple lorsque les victimes sont informées d'une violation de leurs données), alors que la preuve d'autres violations peut être complexe à apporter (conservation des données au-delà des durées prévues, détournement de finalités, manquement à la confidentialité des données…). Par exemple, en ce qui concerne la preuve de l'existence d'un traitement, les juges retiennent une interprétation stricte, peu favorable aux victimes[2152]. Dans plusieurs décisions critiquées, la Cour de cassation

---

[2148] L'article 4 § 12 du règlement UE n° 2016/679 définit la violation de données à caractère personnel comme « une violation de la sécurité, accidentelle ou illicite, entraînant la destruction, la perte, l'altération, la divulgation, ou l'accès non autorisé à de telles données ».
[2149] L'article 9 du code de procédure civile prévoit en effet que « il incombe à chaque partie de prouver conformément à la loi les faits nécessaires au succès de sa prétention » et l'article 1353 du code civil dispose en son alinéa premier que « celui qui réclame l'exécution d'une obligation doit la prouver ».
[2150] Art. 1358 du code civil.
[2151] Cass. civ. 3e, 3 mars 2010, n° 08-21.056, *Bull. civ.* 2010, III, n° 52 ; Cass. civ. 2e, 6 mars 2014, n° 13-14.295, *Bull. civ.* 2014, II, n° 65.
[2152] Sur la difficulté d'établir la preuve de l'existence d'un traitement, v. A. Debet, J. Massot et N. Métallinos, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015, n° 452, p. 199.

a affirmé que cette preuve n'était pas démontrée, alors même que des données à caractère personnel étaient pourtant collectées[2153]. En effet, l'absence de fichier centralisé dans lequel était conservé ces données empêchait, selon la Haute juridiction, de caractériser l'existence d'un traitement. Les difficultés probatoires s'expliquent particulièrement par l'asymétrie informationnelle résultant des traitements de données à caractère personnel.

548. L'asymétrie informationnelle inhérente à la matière. Dans la mesure où ils sont effectués selon la volonté des responsables du traitement, les traitements de données personnelles sont invisibles pour la personne concernée[2154]. Cette dernière est donc rarement dans une position lui permettant de comprendre l'ensemble des aspects relatifs aux traitements effectués sur ses données[2155]. Pour remédier à l'asymétrie entre le responsable du traitement et la personne concernée, le législateur a prévu des obligations d'information à la charge des responsables du traitement, notamment sur l'étendue des données collectées, les finalités des traitements ou les durées de conservation des données[2156]. L'une des principales difficultés liées à ces obligations d'information est qu'elles se traduisent, la plupart du temps, par la fourniture d'informations très générales[2157]. Par exemple, au sujet de la conservation des données, de nombreuses entreprises affirment les conserver jusqu'à ce qu'elles ne soient plus nécessaires pour fournir les services ou produits[2158]. Une telle affirmation empêche la

---

[2153] Cass. soc., 28 nov. 2007, n° 06-21.964, *Bull.* 2007, V, n° 201. V. déjà, Cass. crim., 3 nov. 1987, n° 87-83.429, *Bull. crim.* 1987, n° 382, p. 1007, dans lequel la Cour retenait que « pour relaxer le prévenu du chef d'enregistrement ou conservation de données collectées par des moyens frauduleux, déloyaux ou illicites, les juges retiennent que les renseignements obtenus sur la solvabilité des personnes concernées figuraient dans leur dossier, mais non dans le traitement automatisé d'informations nominatives exploité par X..., ni dans aucun fichier ». Pour une analyse critique de ces décisions, v. not. J.-M. Béraud, « Entretien annuel d'évaluation des salariés, consultation du CHSCT et déclaration auprès de la CNIL », *Le Droit Ouvrier* 2008, p. 49. Pour une critique de l'absence de définition de la notion de fichier dans la loi du 6 janvier 1978, v. J. Frayssinet, « La Cour de cassation et la loi informatique, fichiers et libertés, ou comment amputer une loi tout en raffermissant son application », *JCP G* 1988, I, p. 3323.

[2154] Pour Madame Jessica Eynard, c'est justement parce que ces données « échappent intellectuellement et juridiquement » à la personne concernée qu'elles doivent être qualifiées de données à caractère personnel, v. J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 184.

[2155] S. Vizard, « Despite GDPR, consumers still don't understand how brands use their data », *MarketingWeek* 25 mai 2018.

[2156] Selon Monsieur Yves Poullet, « cette asymétrie, pourtant encore limitée à l'heure des premières législations de protection des données, était déjà à leur base et les justifiait selon les promoteurs de ces législations. Il s'agissait par ces lois de rétablir un certain équilibre à la fois en instaurant la transparence des traitements et en fixant des balises au droit à traiter l'information », Y. Poullet, *La vie privée à l'heure de la société numérique,* Larcier, 2019, n° 20, p. 38.

[2157] Au sujet du caractère vague des finalités déclarées, v. D. Gutmann, *Le sentiment d'identité. Étude de droit des personnes et de la famille*, th. Paris II, 2000, LGDJ, n° 293, p. 253.

[2158] V. par ex., Facebook, « Politique d'utilisation des données. Conservation des données, désactivation et suppression d'un compte », consulté le 29 oct. 2020. L'article 13 du règlement UE n° 2016/679 prévoit quand même que le responsable du traitement doit fournir « la durée de conservation des données à caractère personnel

personne concernée de démontrer que les données ont été conservées au-delà des durées prévues, justement parce que ces durées ne sont pas détaillées[2159].

À ces difficultés pratiques s'ajoutent également les difficultés techniques liées aux traitements de données à caractère personnel. Malgré l'utilisation massive et diffuse de l'informatique, les traitements demeurent encore de véritables « boîtes noires » pour la plupart des personnes concernées, et la preuve des manquements aux obligations prévues par le droit des données à caractère personnel s'avère souvent difficile à apporter. Par exemple, comment la personne concernée peut-elle s'assurer que ses données ne sont pas transmises à des tiers ? Comment peut-elle vérifier le respect des finalités décrites par le responsable du traitement ? Comment la victime d'un taux d'emprunt plus élevé peut-elle apporter la preuve que ce taux est dû à un traitement illicite de ses données personnelles ? Seul l'organisme traitant les données a une connaissance précise et avérée des traitements qu'il effectue. Une asymétrie informationnelle est donc bien caractérisée entre la personne concernée et le responsable du traitement, au bénéfice de ce dernier. Ce déséquilibre affecte les personnes concernées dans leur capacité à prouver des manquements aux obligations résultant du droit des données personnelles.

L'extension des contrôles proposée répond en partie à cette difficulté puisque l'augmentation des moyens de contrôle, notamment internes[2160], permettra sans doute à un plus grand nombre de manquements d'être rendus publics, facilitant ainsi leur preuve. La poursuite plus régulière des infractions prévues par le code pénal, notamment celles liées aux durées de conservation[2161] ou aux transferts de données auprès de tiers[2162], pourrait également contribuer à encourager les responsables du traitement à mieux respecter ces principes. Enfin, la coloration des données, proposée dans la présente étude[2163], pourrait utilement être utilisée afin de montrer les passages

---

ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ». En pratique, il est rare de voir une politique de confidentialité donner la durée précise de conservation des données.

[2159] En 2011, Monsieur Maximilian Schrems avait prouvé la pratique de Facebook consistant à effacer certaines données, uniquement pour l'utilisateur, tout en les conservant dans le système d'information de Facebook, v. M. Schrems, « Complaint against Facebook Ireland Ltd. », *europe-v-facebook.org* 18 août 2011. Un jugement du tribunal de grande instance de Paris a confirmé l'existence de cette pratique, TGI Paris, 9 avr. 2019, *UFC-Que Choisir* c. *Facebook*, nº 14/07928, p. 37. Dans cette situation, il est d'ailleurs possible de se demander si la responsabilité civile à engager ne serait pas de nature contractuelle, particulièrement si des engagements particuliers ont été pris dans le contrat, v. E. Netter, « L'extinction du contrat et le sort des données personnelles », *AJ Contrat* 2019, p. 416.

[2160] V. *supra*, nº 505.

[2161] Art. 226-20 du code pénal. Cet article fait toutefois référence à la durée de conservation déclarée auprès de la CNIL, une modification législative serait donc nécessaire pour prendre en compte l'évolution vers le régime de responsabilité et retirer la référence à la déclaration.

[2162] Art. 226-22 du code pénal.

[2163] V. *supra,* nº 440.

empruntés par les données, et éventuellement prouver des transmissions de données à des tiers. Toutefois, ces propositions, bien que nécessaires, ont des effets limités, et il semble qu'une révision plus profonde du régime de la preuve de la faute soit nécessaire. D'autres difficultés probatoires existent à l'occasion de la preuve du préjudice.

B. Le préjudice

549. Les caractères du préjudice. Classiquement, pour être considéré comme réparable, le préjudice doit présenter plusieurs caractères : il doit être direct, personnel et certain[2164]. Un préjudice est direct lorsqu'il a été causé par le fait dommageable[2165]. Cette exigence renvoie, de fait, à la notion de causalité et souligne l'exigence d'un lien de causalité entre le préjudice et le fait allégué[2166]. Le caractère personnel du préjudice apparaît dans l'intérêt à agir du demandeur[2167]. Enfin, le préjudice doit être certain, c'est-à-dire non éventuel ou hypothétique[2168].

550. La distinction entre le dommage et le préjudice. La plupart des auteurs s'accordent pour distinguer le dommage du préjudice : le dommage serait une notion purement matérielle, représentant l'atteinte de fait, alors que le préjudice renverrait à une notion juridique, désignant les conséquences de cette atteinte[2169]. Cette distinction est critiquée par une partie de la doctrine[2170], notamment parce qu'elle serait artificielle lorsque le siège de l'atteinte n'a pas d'existence physique, comme c'est le cas pour les droits de la personnalité[2171]. Si, dans certains cas, cette distinction n'est pas très utile,

---

[2164] P. Malaurie, L. Aynès et P. Stoffel-Munck, *Droit des obligations*, 10e éd., LGDJ, 2018, no 241, p. 146. Pour Monsieur Philippe Brun, le préjudice, pour donner lieu à réparation, doit être « actuel, direct et certain », v. P. Brun, *Responsabilité civile extracontractuelle*, 5e éd., LexisNexis, 2018, no 179, p. 124. La jurisprudence avait parfois recours au critère de légitimité du dommage, notamment dans le but d'exclure certaines demandes en réparation, sur ce point, v. not. M. Bacache-Gibelli, *La responsabilité civile extracontractuelle,* 3e éd., Economica, 2016, nos 398 s., p. 466 ; F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, nos 927 s., p. 1010 s.

[2165] S. Porchy-Simon, *Droit civil 2e année. Les obligations,* 10e éd., Dalloz, 2017, no 935, p. 446.

[2166] F. Terré, P. Simler, Y. Lequette et F. Chénedé, *Droit civil. Les obligations,* 12e éd., Dalloz, 2018, no 926, p. 1009.

[2167] P. Malaurie, L. Aynès et P. Stoffel-Munck, *Droit des obligations*, 10e éd., LGDJ, 2018, no 241, p. 146.

[2168] M. Bacache-Gibelli, *La responsabilité civile extracontractuelle,* 3e éd., Economica, 2016, no 374, p. 425.

[2169] V. not. J.-S. Borghetti, « Les intérêts protégés et l'étendue des préjudices réparables en droit de la responsabilité civile extra-contractuelle », in *Mélanges G. Viney*, LGDJ, 2008, p. 145 s., spéc. p. 149 s. ; S. Rouxel, *Recherches sur la distinction du dommage et du préjudice,* th. Grenoble, 1994. V. aussi, N. Dejean de la Bâtie, *Droit civil français*, t. VI-2, dir. C. Aubry et C. Rau, 8e éd., Litec, 1989, no 10, p. 19 ; A. Guégan-Lécuyer, *Dommages de masse et responsabilité civile*, th. Paris I, 2006, LGDJ, nos 60 s., p. 68 s.

[2170] V. not. G. Durry, « Rapport de synthèse », in *Le préjudice : questions choisies. Responsabilité civile et assurances* 1998, no 5, p. 32 ; M. Fabre-Magnan, *Droit des obligations,* t. 2, *Responsabilité civile et quasi-contrats*, 4e éd., PUF, 2019, no 104, p. 132 s.

[2171] F. Leduc, « Faut-il distinguer le dommage et le préjudice ? : point de vue privatiste », *Responsabilité civile et assurances* 2010, no 3, dossier 3, § 6. Pour une opinion contraire, v. L. Gratton, « Le dommage déduit de la faute », *RTD civ.* 2013, p. 275.

elle l'est en droit des données à caractère personnel. En effet, dans cette matière la distinction met en exergue la double difficulté à laquelle est confrontée la victime. Cette dernière rencontre des difficultés non seulement à l'occasion de la preuve du dommage (1), mais aussi lors de l'évaluation du préjudice (2).

1. La preuve du dommage

551. Le dommage. L'existence d'un dommage est un principe essentiel de la responsabilité civile[2172]. Dans la plupart des cas de responsabilité, c'est une condition déterminante puisque sa survenance justifie la demande en indemnisation ou en cessation du manquement[2173]. Selon une formule établie de la Cour de cassation, « le propre de la responsabilité civile est de rétablir aussi exactement que possible l'équilibre détruit par le dommage et de replacer la victime dans la situation où elle se serait trouvée si l'acte dommageable ne s'était pas produit »[2174]. Cette indemnisation résulte de la comparaison entre ces deux situations[2175]. Il s'agit donc de rendre ce qui a été perdu, de sorte que la victime soit finalement indemne du dommage[2176].

552. La difficulté de prouver le dommage en cas d'atteinte aux droits de la personnalité. Plusieurs difficultés sont susceptibles d'entraver l'action en responsabilité de la victime d'une atteinte aux droits de sa personnalité. L'une des difficultés les plus évidentes est celle relative à la preuve de son dommage.

[2172] P. Brun, *Responsabilité civile extracontractuelle*, 5e éd., LexisNexis, 2018, no 175, p. 119. Si la fonction indemnitaire est centrale dans la responsabilité, les fonctions préventive et punitive y trouvent une place croissante. En témoigne, par exemple, le projet de réforme de la responsabilité civile qui prévoit, dans son chapitre IV, que le juge peut prescrire les mesures propres à prévenir le dommage et qui introduit un mécanisme général d'amende civile, Ministère de la Justice, « Projet de réforme de la responsabilité civile », mars 2017 ; v. les propositions d'articles 1266 et 1266-1 du code civil. Pour une analyse de la meilleure prise en compte de ces fonctions par le projet de réforme de la responsabilité civile, v. not. N. Rias, « Regard français », in *Quel avenir pour la responsabilité civile ?,* dir. Y. Lequette et N. Molfessis, Dalloz, 2017, p. 63 s. Le Sénat, dans une proposition de loi portant réforme de la responsabilité civile, reprend également ces dispositions, proposition de loi de Messieurs Philippe Bas (*et al.*) et Mesdames Catherine André (*et al.*) portant réforme de la responsabilité civile, Sénat, no 678, déposée le 29 juill. 2020. Pour un exposé de cette évolution, v. J. Rochfeld, *Les grandes notions du droit privé*, 2e éd., PUF, 2013, *Vo* « Le contrat », nos 12 s. p. 496 s.

[2173] S. Porchy-Simon, *Droit civil 2e année. Les obligations,* 10e éd., Dalloz, 2017, no 922, p. 444.

[2174] V. parmi les très nombreux arrêts, Cass. civ. 2e, 28 oct. 1954, *JCP* 1955, p. 8765 ; Cass. civ. 2e, 19 nov. 1975, no 74-13.018, *Bull. civ.* II, no 302, p. 243.

[2175] G. Viney, P. Jourdain et S. Carval, *Les effets de la responsabilité,* 4e éd., LGDJ, 2017, no 116, p. 153. Comme le remarque très justement Monsieur Jean-Baptiste Prévost, la réparation « n'est pas un supplément, un excès, un excédent, mais une manière de rétablir l'intégrité brisée ; de rétablir ce qui n'aurait pas dû être détruit », J.-B. Prévost, « Aspects philosophiques de la réparation intégrale », *Gaz. Pal.* 2010, no 100, p. 7.

[2176] P. Malaurie, L. Aynès et P. Stoffel-Munck, *Droit des obligations*, 10e éd., LGDJ, 2018, no 238, p. 143. La jurisprudence rappelle régulièrement que le préjudice doit être intégralement réparé, sans qu'il résulte pour la victime ni perte ni profit, v. parmi les nombreux arrêts, Cass. civ. 2e, 23 janv. 2003, no 01-00.200, *Bull. civ.* 2003, II, no 20, p. 16.

Pourtant, en 1971, au sujet de l'atteinte à la vie privée, Roger Nerson minimisait cette difficulté en considérant qu'il « ne faudrait pas exagérer l'importance de ce fardeau »[2177]. Selon lui, la ligne de démarcation entre la justification d'un intérêt à agir et la démonstration d'un dommage moral subi par le demandeur serait ténue : dans la quasi-totalité des procès, l'information publiée ou l'image reproduite porte atteinte à l'honneur ou à la considération de la personne concernée[2178]. Cette parenté entre l'intérêt à agir et le dommage explique que, pour le droit au respect de la vie privée, la jurisprudence s'est orientée vers un principe de présomption de dommage et a instauré un caractère automatique entre l'atteinte et la caractérisation du préjudice[2179]. La doctrine a décelé dans cette évolution la reconnaissance d'un véritable droit subjectif[2180]. Ainsi, toute atteinte à ce droit constitue *ipso facto* une violation du droit au respect de la vie privée caractérisant un dommage, au moins moral[2181]. Toutefois, l'automaticité entre l'utilisation d'une donnée à caractère personnel et l'atteinte à la personne est loin d'être aussi systématique que celle existant pour le droit au respect de la vie privée.

553. La difficulté de prouver le dommage en cas d'atteinte aux données personnelles. La présomption établie par l'article 9 du code civil n'est pas reconnue pour les victimes d'atteinte aux données personnelles qui doivent, elles, prouver l'existence de leurs dommages[2182]. Cette preuve peut s'avérer difficile à apporter pour les victimes. Tout d'abord, la victime peut être dans l'ignorance des manquements au droit des données personnelles et ainsi ne pas avoir conscience des dommages qu'elle

---

[2177] R. Nerson, « La protection de la vie privée en droit positif français », *RID comp.* 1971, vol. 23, nº 4, p. 737, § 27, spéc. p. 757.
[2178] R. Nerson, « Jurisprudence française en matière de droit civil », *RTD civ.* 1968, p. 533, spéc. p. 539 et R. Nerson, « La protection de la vie privée en droit positif français », *RID comp.* 1971, vol. 23, nº 4, p. 737, § 27, spéc. p. 757.
[2179] G. Viney et P. Jourdain, *Les conditions de la responsabilité*, 4e éd., LGDJ, 2013, nº 247-3, p. 10 ; M. Bacache-Gibelli, *La responsabilité civile extracontractuelle,* 3e éd., Economica, 2016, nº 424, p. 502. V. par ex., Cass. civ. 1re, 5 nov. 1996, nº 94-14.798, *Bull. civ.* 1996, I, nº 378, p. 265 ; v. aussi, Cass. civ. 2e, 24 mars 2016, nº 14-29.519, *NPB*.
[2180] R. Nerson, « Jurisprudence française en matière de droit civil », », *RTD civ.* 1966, p. 65, spéc. p. 66 ; R. Badinter, « Le droit au respect de la vie privée », *JCP G* 1968, I, doctr. 2136, nº 24 ; P. Kayser, « Le secret de la vie privée et la jurisprudence civile », in *Mélanges R. Savatier*, Dalloz, 1965, p. 405 s., nos 7 s., spéc. p. 411 s. Plus récemment, v. not. S. Laulom, « L'indépendance affirmée de l'article 9 du code civil du droit commun de la responsabilité », *D.* 1997, p. 403 ; J.-C. Saint-Pau, « La distinction des droits de la personnalité et de l'action en responsabilité civile », in *Mélanges H. Groutel*, Litec, 2006, p. 405 s., nº 10, spéc. p. 412 ; P. Jourdain, « Les droits de la personnalité à la recherche d'un modèle : la responsabilité civile », *Gaz. Pal.* 2007, nº 139, p. 52 ; L. Gratton, « Le dommage déduit de la faute », *RTD civ.* 2013, p. 275.
[2181] V. *infra,* nº 557. V. aussi, G. Goubeaux, *Traité de droit civil. Les personnes*, LGDJ, 1989, nos 274 s., p. 247 s. ; S. Laulom, « L'indépendance affirmée de l'article 9 du code civil du droit commun de la responsabilité », *D.* 1997, p. 403 ; J. Ravanas, « Le plein exercice du droit au respect de la vie privée », *D.* 1998, p. 474, nº 7.
[2182] Art. 82 du règlement UE nº 679/2016.

subit. Par exemple, si un responsable du traitement traite des données dans l'objectif de manipuler une personne afin qu'elle effectue certains achats, cette victime n'aura sans doute pas pleinement conscience de cette manipulation. Pour autant, il est désormais établi que l'état d'inconscience de la victime n'empêche pas la réalisation du préjudice[2183]. Ensuite, ces manquements peuvent causer un dommage difficile à cerner. Déjà en 1984 au sujet de l'information, Pierre Catala énonçait que « le dommage causé par l'appréhension ou la diffusion indue d'une information risque de se révéler souvent difficilement réparable »[2184]. Par exemple, si un responsable du traitement communique des données à des tiers non autorisés, quelle est la nature du dommage en résultant ? Quelle est la nature du dommage résultant du refus, par un responsable du traitement, de laisser la personne concernée accéder à ses données ?

Enfin, le caractère subjectif des atteintes résultant de ces manquements complexifie encore davantage l'établissement de leur preuve. Même si les personnes ressentent ces atteintes de manière différente, les juges devront tout de même faire preuve de cohérence dans l'appréciation de ces dommages. C'est d'ailleurs l'une des raisons qui poussent le juge américain à s'intéresser à la notion de « *reasonable expectation of privacy* », c'est-à-dire à ce qui est classiquement attendu dans une certaine situation[2185]. Toutes ces difficultés probatoires sont exacerbées lorsqu'il s'agit d'évaluer le préjudice.

2. L'évaluation du préjudice

554. Les types de préjudice. Le principe de réparation intégrale du préjudice implique que la victime a le droit d'être indemnisée de toutes les atteintes causées par le fait dommageable. La liste des préjudices indemnisables est donc immense, tant les conséquences d'un dommage peuvent être variées. Historiquement, la doctrine opposait

---

[2183] Sur le lien entre le caractère réparable des préjudices et l'inconscience de la victime pouvant se représenter le dommage, notamment pour les victimes se trouvant dans le coma, v. Cass. crim., 5 janv. 1994, nº 93-83.050, *Bull. crim.* 1994, nº 5, p. 8, selon laquelle « l'indemnisation d'un dommage n'est pas fonction de la représentation que s'en fait la victime mais de sa constatation par le juge et de son évaluation objective ». Pour un exposé des thèses subjectivistes et objectivistes en la matière, v. C. Bloch, *Droit de la responsabilité et des contrats*, Dalloz Action, 2018-2019, nº 2125.31.

[2184] P. Catala, « Ébauche d'une théorie juridique de l'information », *D.* 1984, p. 97, nº 10.

[2185] Pour des analyses de cette notion, v. R. Wilkins, « Defining the "reasonable expectation of privacy" : an emerging tripartite analysis », *Vanderbilt Law Review* 1987, vol. 40, p. 1077 s. [40 VAND. L. REV. 1077] ; S. Spencer, « Reasonable expectations and the erosion of privacy », *San Diego Law Review* 2002, vol. 39, p. 843 s. [39 SAN DIEGO L. REV. 843] ; L. Serafino, « Arguing for protection of data stored in the cloud », *Pennyslvania Lawyer* 2013, vol. 35, p. 28 s. [45 PA. LAW 28].

le dommage matériel au dommage moral[2186]. Le premier était défini comme le dommage portant atteinte au patrimoine d'une personne[2187], alors que le second visait le dommage affligé aux attributs extrapatrimoniaux de la personne (considération, honneur, réputation), à la personnalité morale (croyances, convictions, pudeur), aux sentiments ou à l'agrément de vie (mort d'un être cher, rupture de fiançailles, gêne sexuelle)[2188]. Cette ramification, jugée approximative et présentant des inconvénients[2189], a laissé place à la *summa divisio* distinguant les préjudices patrimoniaux des préjudices extrapatrimoniaux[2190]. Cette distinction est utile pour comprendre les types de préjudices pouvant être indemnisés en cas de manquement aux obligations prévues par le droit des données à caractère personnel.

555. Les préjudices patrimoniaux. Le préjudice patrimonial correspond à toute atteinte aux intérêts économiques de la victime qui peut consister tant dans une perte éprouvée qu'en un gain manqué[2191]. Le plus souvent, le préjudice patrimonial résulte d'un dommage corporel ou d'une atteinte aux biens[2192]. Cette dernière se traduit par un préjudice matériel consistant dans la perte ou la détérioration d'une chose[2193] ; quant au dommage corporel, c'est celui portant atteinte à l'intégrité physique[2194]. De nombreux chefs d'indemnisation découlent de ces préjudices patrimoniaux. En matière d'atteintes aux biens, il s'agit par exemple de la diminution ou de la perte de la valeur vénale du bien, des troubles de jouissance ou encore de la perte des profits pouvant résulter de l'usage du bien[2195] ; en matière d'atteinte à la personne, on identifie par

[2186] V. déjà en ce sens M. Planiol, *Traité élémentaire de droit civil*, t. 2, 11e éd., LGDJ, 1931, no 247, p. 97. La reconnaissance du dommage moral ne s'est pas faite sans difficulté, v. F. Givord, *La réparation du préjudice moral*, th. Grenoble, 1938, Dalloz. Cette opposition était présente dans la jurisprudence, v. l'arrêt précurseur Cass. ch. réun., 25 juin 1833, *Sirey* 1833, I, p. 458, et surtout les conclusions du procureur général A. Dupin. Pour la consécration de cette distinction, v. Cass. civ., 13 févr. 1923, *Lejars* c. *Consorts Templier*.
[2187] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vo* « Dommage », sens 2, spéc. matériel.
[2188] Art. 3 du code de procédure pénale et S. Guinchard et T. Debard (dir.), *Lexique des termes juridiques*, 27e éd., Dalloz, 2019-2020, *Vo* « Dommage moral ».
[2189] H., L. et J. Mazeaud et F. Chabas, *Leçons de droit civil,* t. 2, vol. I, *Obligations*, 9e éd., par F. Chabas, Montchrestien, 1998, no 417, p. 422 ; v. aussi, B. Starck, H. Roland et L. Boyer, *Obligations*, vol. I, *Responsabilité délictuelle*, 5e éd., Litec, 1996, no 104, p. 56 et no 114, p. 66.
[2190] C'est d'ailleurs celle retenue par la nomenclature proposée par Jean-Pierre Dintilhac et reprise par les nomenclatures postérieures, J.-P. Dintilhac (dir.), « Rapport du groupe de travail chargé d'élaborer une nomenclature des préjudices corporels », juill. 2005.
[2191] P. Brun, *Responsabilité civile extracontractuelle*, 5e éd., LexisNexis, 2018, no 212, p. 146.
[2192] M. Bacache-Gibelli, *La responsabilité civile extracontractuelle,* 3e éd., Economica, 2016, no 425, p. 503.
[2193] Sur la diminution de la valeur, v. Cass. civ. 2e, 30 janv. 1985, no 83-12.029, *Bull. civ.* 1985, II, no 24, p. 16 ; Cass. civ. 2e, 17 mai 1995, no 93-15.183, *Bull. civ.* 1995, II, no 142, p. 81.
[2194] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vo* « Dommage », sens 2, spéc. corporel.
[2195] P. Brun, *Responsabilité civile extracontractuelle*, 5e éd., LexisNexis, 2018, no 213, p. 146.

exemple les dépenses de santé, la perte de gains professionnels, les frais de logement adapté, ou encore l'assistance nécessaire résultant du dommage[2196].

556. Les préjudices extrapatrimoniaux. Défini comme l'atteinte au bien-être de la victime[2197], son « déplaisir » selon la formule de René Savatier[2198], le préjudice extrapatrimonial a longtemps fait l'objet de contestations doctrinales, particulièrement sur la question de son caractère réparable[2199]. Les termes du plaidoyer sont connus : comment l'octroi d'une somme d'argent pourrait réparer « l'irréparable »[2200] ? Selon certains auteurs, indemniser le préjudice extrapatrimonial encouragerait l'indécence des victimes à venir monnayer leurs larmes devant les prétoires[2201]. Par ailleurs, selon ces auteurs, l'évaluation de ce préjudice a nécessairement un caractère arbitraire puisque la douleur n'a pas de prix[2202]. C'est pourquoi une partie de la doctrine considère que la réparation du préjudice moral, par nature incalculable, revient en pratique à infliger à l'auteur du dommage une *peine privée* à titre, non pas de réparation, mais de sanction[2203].

Les discussions autour du caractère réparable du préjudice extrapatrimonial se sont progressivement apaisées, et la jurisprudence reconnaît désormais un principe

---

[2196] J.-P. Dintilhac (dir.), « Rapport du groupe de travail chargé d'élaborer une nomenclature des préjudices corporels », juill. 2005.
[2197] L. Cadiet, *Le préjudice d'agrément*, th. Poitiers, 1983, n° VII.
[2198] R. Savatier, *Traité de la responsabilité civile en droit français,* t. 2, 2e éd., LGDJ, 1951, p. 95, n° 530.
[2199] V. sur cette controverse, H. et L. Mazeaud et A. Tunc, *Traité théorique et pratique de la responsabilité civile*, t. 1, 6e éd., Montchrestien, 1965, nos 304 s., p. 471 s. Pour des études sur la réparation du préjudice moral, v. not. F. Givord, *La réparation du préjudice moral*, th. Grenoble, 1938, Dalloz ; H. Gali, *Le préjudice moral en droit de la responsabilité civile,* th. Paris-Saclay, 2019.
[2200] M. Fabre-Magnan, « Le dommage existentiel », *D.* 2010, p. 2376. H. et L. Mazeaud et A. Tunc, *Traité théorique et pratique de la responsabilité civile*, t. 1, 6e éd., Montchrestien, 1965, nos 304 s., p. 471 s.
[2201] V. not. L. Josserand, « La personne humaine dans le commerce juridique », *D.* 1932, chron. 1. Pour Paul Esmein « la douleur, certes, peut être profonde, mais on l'avilit en la monnayant », P. Esmein, « La commercialisation du dommage moral », *D.* 1954, chron. 113 ; R. Savatier, *Traité de la responsabilité civile en droit français,* 2e éd., LGDJ, 1951, n° 527, p. 93.
[2202] J. Flour, J.-L. Aubert et E. Savaux, *Droit civil. Les obligations,* t. 2, *Le fait juridique,* 14e éd., Sirey, 2011, n° 388, p. 503.
[2203] G. Ripert, *La règle morale dans les obligations civiles*, 4e éd., LGDJ, 1949, nos 185 s., p. 381 ; G. Ripert, « Le prix de la douleur », *D.* 1948, chron. 1 ; S. Carval, *La responsabilité civile dans sa fonction de peine privée,* th. Paris I, 1995, LGDJ, nos 22 s. et nos 118 s. ; D. Chauvet, *La vie privée. Étude de droit privé,* th. Paris-Sud, 2014, n° 395, p. 330. V. aussi, J. Flour, J.-L. Aubert et E. Savaux, *Droit civil. Les obligations,* t. 2, *Le fait juridique,* 14e éd., Sirey, 2011, n° 388, p. 503 ; P. Malaurie, L. Aynès et P. Stoffel-Munck, *Droit des obligations*, 10e éd., LGDJ, 2018, n° 248, p. 153. Pour une critique de cette conception, v. N. Molfessis, « La réparation du préjudice extrapatrimonial », in *Les limites de la réparation du préjudice*, dir. F. Ewald *et al.*, Dalloz, 2009, p. 395 s., n° 27, p. 412.

général de réparation de celui-ci[2204], ce qui est d'autant plus justifié à l'heure où l'on reconnaît le préjudice moral des personnes morales[2205].

557. La variété des préjudices résultant d'une atteinte aux droits de la personnalité. Aux préjudices moraux classiquement admis, tels que l'atteinte à l'honneur, à la considération, à l'affection ou à un élément de la joie de vivre d'une personne[2206], doivent être ajoutés les préjudices résultant d'une atteinte aux droits de la personnalité[2207]. Comme le relève Monsieur Nicolas Molfessis, si certaines atteintes aux droits de la personnalité peuvent être à l'origine de préjudices patrimoniaux, on sait que le dommage dont se plaint la victime est généralement d'ordre moral[2208]. D'ailleurs, lorsqu'en 1968, Monsieur Robert Badinter plaidait pour la consécration juridique du droit au respect de la vie privée, il affirmait sans détour que « le préjudice causé par une atteinte à la vie privée est évidemment d'ordre moral »[2209]. La violation d'un droit de la personnalité entraîne naturellement un préjudice extrapatrimonial pour la personne qui en est titulaire[2210], pouvant, dans certains cas, être accompagné d'un préjudice patrimonial[2211]. Les préjudices résultant des manquements au droit des données personnelles n'échappent pas à cette règle[2212].

558. La difficulté d'évaluer le préjudice en matière d'atteinte aux données à caractère personnel. La détermination du *quantum* du préjudice présente également ses propres difficultés[2213]. En 1965, Pierre Kayser s'interrogeait déjà sur

---

[2204] Depuis d'anciens arrêts de la Cour de cassation et du Conseil d'État, les jurisprudences judiciaires et administratives sont constantes, v. Cass. ch. réun., 15 juin 1833, *Sirey* 1833, I, p. 458 et CE Ass., 24 nov. 1961, *Ministre des travaux publics* c. *Latisserand*, n° 48841, *Lebon* p. 661.
[2205] V. not. V. Wester-Ouisse, « Le préjudice moral des personnes morales », *JCP G* 2003, n° 26, doctr. 145 ; P. Stoffel-Munck, « Le préjudice moral des personnes morales », in *Mélanges P. le Tourneau*, 2008, p. 959 s., n^{os} 3, spéc. p. 960 s. La jurisprudence accueille ce préjudice, v. not. Cass. com., 9 févr. 1993, n° 91-12.258, *Bull. civ.* 1993, IV, n° 53 ; Cass. com., 15 mai 2012, n° 11-10.278, *Bull.* 2012, IV, n° 101.
[2206] G. Cornu (dir.), *Vocabulaire juridique*, 13^{e} éd., PUF, 2020, *V°* « Dommage », sens 2, spéc. moral.
[2207] Pour une étude approfondie de la réparation du préjudice extrapatrimonial résultant d'une atteinte aux droits de la personnalité, v. P. Le Tourneau (dir.), *Droit de la responsabilité et des contrats. Régimes d'indemnisation*, 11^{e} éd., Dalloz Action, 2018-2019, n° 2125.191.
[2208] N. Molfessis, « La réparation du préjudice extrapatrimonial », in *Les limites de la réparation du préjudice*, dir. F. Ewald *et al.*, Dalloz, 2009, p. 395 s., n° 29, p. 414.
[2209] R. Badinter, « Le droit au respect de la vie privée », *JCP G* 1968, I, doctr. 2136, n° 30.
[2210] M. Bacache-Gibelli, *La responsabilité civile extracontractuelle,* 3^{e} éd., Economica, 2016, n° 424, p. 502.
[2211] N. Molfessis, « La réparation du préjudice extrapatrimonial », in *Les limites de la réparation du préjudice*, dir. F. Ewald *et al.*, Dalloz, 2009, p. 395 s., n° 29, p. 414. V. aussi, *Rép. civ.* Dalloz, *V°* « Personnalité (Droits de la) », par A. Lepage, 2009 (actu. 2020), n^{os} 265 s.
[2212] Sur les types de préjudice, v. *infra*, n° 572.
[2213] Déjà en 1929, les auteurs d'une note publiée dans la *Harvard Law Review* relevaient la grande difficulté liée à la quantification, sur une échelle pécuniaire, du dommage lié aux violations de la *privacy*, v. Notes, « The right to privacy today », *Harvard Law Review* 1929, vol. 43, p. 297 s. [43 HARV. L. REV. 297], spéc. p. 299.

l'indemnisation de l'atteinte au droit au respect de la vie privée[2214]. Comment quantifier une atteinte qui se prête si mal à l'évaluation ? Comment calculer l'incalculable[2215] ? Selon une opinion doctrinale, un consensus se serait cristallisé sur l'idée qu'il n'est pas possible de réparer, au sens classique du terme, le dommage moral[2216]. L'atteinte causée par ce dommage est irréversible et la remise en état est donc inconcevable. Pourtant, lorsque les juges sont saisis, ils sont tenus d'évaluer le préjudice[2217]. Ainsi, le dommage résultant d'une atteinte aux droits de la personnalité ne relève pas d'une simple opération de constat mais d'une construction juridique relevant de l'appréciation du juge[2218]. Cette évaluation se fait plutôt de manière subjective : les juges recherchent la souffrance ressentie par les victimes, différente pour chacune d'elles[2219]. Cette appréciation fait régulièrement l'objet de critiques et est souvent taxée d'arbitraire[2220], d'autant que l'appréciation du préjudice relève du pouvoir souverain des juges du fond et n'est donc pas contrôlée par la Cour de cassation[2221]. Certains auteurs n'hésitent pas à affirmer que cette évaluation de l'indemnité révèlerait d'une tendance jurisprudentielle sanctionnant la faute déloyale ou lucrative[2222].

En matière de données à caractère personnel, l'atteinte est souvent diffuse et l'évaluation d'un préjudice clairement identifié peut être difficile à apporter. Comme le remarquait Monsieur Fabrice Mattatia, « sauf dans les cas d'escroquerie suite à un *phishing*, les préjudices sont difficiles à chiffrer, voire totalement virtuels »[2223].

[2214] P. Kayser, « Le secret de la vie privée et la jurisprudence civile », in *Mélanges R. Savatier*, Dalloz, 1965, p. 405 s., nº 11, spéc. p. 416 s. V. aussi, G. Ripert, « Le prix de la douleur », *D.* 1948, chron. 1.

[2215] L'expression est empruntée à Monsieur Alain Supiot qui l'utilise notamment à l'égard de la dignité humaine, A. Supiot, *La gouvernance par les nombres. Cours au Collège de France (2012-2014)*, Fayard, 2015, p. 183 s., et p. 202 s.

[2216] N. Molfessis, « La réparation du préjudice extrapatrimonial », in *Les limites de la réparation du préjudice*, dir. F. Ewald *et al.*, Dalloz, 2009, p. 395 s., nº 26, p. 412.

[2217] L'article 4 du code civil prévoit en effet que « le juge qui refusera de juger, sous prétexte du silence, de l'obscurité ou de l'insuffisance de la loi, pourra être poursuivi comme coupable de déni de justice ».

[2218] F. Leduc, « Faut-il distinguer le dommage et le préjudice ? : point de vue privatiste », *Responsabilité civile et assurances* 2010, nº 3, dossier 3, § 10. Pour Daniel Amson, cinq critères seraient pris en compte dans l'indemnisation des atteintes à la vie privée, D. Amson, « L'indemnisation du préjudice résultant des atteintes à la vie privée », *Légipresse* 2002, nº 195, p. 128.

[2219] M. Fabre-Magnan, « Le dommage existentiel », *D.* 2010, p. 2376. Lorsque la victime est en état végétatif, l'évaluation retrouve son caractère objectif, v. aussi M. Bacache-Gibelli, *La responsabilité civile extracontractuelle,* 3e éd., Economica, 2016, nº 376, p. 428 ; S. Porchy-Simon, « L'utilisation des barèmes en droit du dommage corporel », in *Le droit mis en barème ?,* dir. I. Sayn, Dalloz, 2014, p. 201 s., spéc. p. 205.

[2220] R. Badinter, « Le droit au respect de la vie privée », *JCP G* 1968, I, doctr. 2136, nº 30.

[2221] N. Molfessis, « La réparation du préjudice extrapatrimonial », in *Les limites de la réparation du préjudice*, dir. F. Ewald *et al.*, Dalloz, 2009, p. 395 s., nº 31, p. 415 ; v. par ex. Cass. soc., 7 nov. 2018, nº 17-16.799, *NPB*. Seuls l'assiette du préjudice et la méthode d'évaluation sont contrôlées par la Cour de cassation, v. P. Malaurie, L. Aynès et P. Stoffel-Munck, *Droit des obligations*, 10e éd., LGDJ, 2018, nº 238, p. 144.

[2222] Sur la faute lucrative, v. not. D. Fasquelle, « L'existence des fautes lucratives », *LPA* 20 nov. 2002, nº 232, p. 27 ; J. Méadel, « Faut-il introduire la faute lucrative en droit français ? », *LPA* 17 avr. 2007, nº 77, p. 6. Sur la fonction normative de la responsabilité civile et la faute lucrative, v. C. Dubois, *Responsabilité civile et responsabilité pénale. À la recherche d'une cohérence perdue,* th. Paris II, 2014, LGDJ, nº 28, p. 33 s.

[2223] F. Mattatia, *La protection des données à caractère personnel face aux usages illicites, déloyaux et frauduleux,* th. Paris X, 2010, p. 366.

L'évaluation des préjudices est d'autant plus complexe qu'ils peuvent s'étaler sur une longue durée[2224]. Par exemple, une fuite de données peut engendrer une usurpation d'identité[2225] ou un refus d'embauche[2226] se réalisant des mois, voire des années après le constat de la violation de données. Les preuves de la faute, du préjudice, ainsi que son *quantum* se révèlent donc difficiles à établir pour la victime, et une simplification de la réparation est donc nécessaire.

§ II. *De lege ferenda* : la simplification de l'action en responsabilité

559. Plan. Le souci de protéger des droits non pas théoriques ou illusoires mais concrets et effectifs passe nécessairement par la reconnaissance d'actions en défense des droits reconnus[2227]. Ces actions doivent être fonctionnelles et permettre à toute personne s'estimant victime d'agir en justice. Pour favoriser les actions en responsabilité et garantir aux victimes une certaine sécurité juridique, une simplification de la réparation semble nécessaire. Celle-ci passe notamment par l'établissement d'une présomption simple de faute (A), ainsi que par la création d'une nomenclature des préjudices résultant des manquements au droit des données personnelles (B).

[2224] En principe, le juge doit évaluer le préjudice au moment où il statue : v. P. Malaurie, L. Aynès et P. Stoffel-Munck, *Droit des obligations*, 10e éd., LGDJ, 2018, nos 252 s., p. 155 s. Dans un arrêt de 1983, la Cour de cassation a rappelé le principe selon lequel « si le droit, pour la victime d'un accident, d'obtenir la réparation du préjudice subi existe dès que le dommage a été causé, l'évaluation de ce dommage doit être faite par le juge au moment où il rend sa décision », Cass. civ. 2e, 21 mars 1983, no 82-10.770, *Bull. civ.,* II no 88. Ce principe s'applique également aux atteintes aux droits de la personnalité, v. not. A. Lepage, « Précisions sur les modes de réparation du préjudice en matière d'atteintes à la vie privée et à l'image », *D.* 2003, p. 1542.

[2225] En vertu de l'article 226-4 du code pénal, l'usurpation d'identité consiste à « usurper l'identité d'un tiers ou [à] 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 ». Pour des analyses du délit d'usurpation d'identité, v. not. T. Cassuto, « Usurpation d'identité numérique », *AJ pénal* 2010, p. 220 ; M. Monteil, « L'usurpation d'identité à l'épreuve du numérique », *D.* 2020, p. 101.

[2226] Lorsqu'il est discriminatoire, le refus d'embauche est un délit pénal, sanctionné par les articles 225-2 et suivants du code pénal. La notion de refus d'embauche a été précisée notamment dans un arrêt de la chambre criminelle de la Cour de cassation du 2 septembre 2003. Pour la Cour, « le refus, par une société recourant aux services d'une entreprise de travail temporaire, de conclure le contrat de mise à disposition prévu par l'article L. 124-3 du code du travail constitue un refus d'embauche au sens de l'article 225-2, 3 du code pénal dès lors qu'il fait obstacle à l'embauche, par l'entreprise de travail temporaire, du salarié visé dans le contrat », v. Cass. crim., 2 sept. 2003, no 02-86.048, *Bull. crim.* 2003, no 148, p. 593. Plus généralement, v. *Rép. trav.* Dalloz, *Vo* « Discrimination », par M.-T. Lanquetin, 2010 (actu. 2020), nos 422 s.

[2227] Sur l'effectivité des droits, v. not. CEDH, 9 oct. 1979, *Airey* c. *Irlande,* no 6289/73, § 24. Pour une analyse de l'effectivité des droits selon la CEDH, B. Delzangles, « Effectivité, efficacité et efficience dans la jurisprudence de la Cour européenne des droits de l'homme », in *À la recherche de l'effectivité des droits de l'homme*, dir. V. Champeil-Desplats et D. Lochak, Presses Universitaires de Paris Ouest, 2008, p. 41.

A. L'établissement d'une présomption simple de faute

560. L'articulation entre le domaine de la vie privée et celui des données personnelles. Certaines des atteintes engendrées par des violations du droit des données personnelles ont vocation à être sanctionnées tant par le droit des données personnelles que par le droit pénal ou le droit civil, notamment sur le fondement du droit au respect de la vie privée. Pour la plupart de ces atteintes, l'action fondée sur l'article 9 du code civil pourrait être privilégiée, en raison de ses conditions favorables aux victimes. En effet, la seule constatation d'une atteinte à la vie privée ouvre droit à réparation et oblige le juge à réparer le préjudice subi[2228].

Toutefois, toutes les atteintes aux données à caractère personnel ne sont pas réparables sur le fondement du droit au respect de la vie privée. Pour cela, il faut que les données en question entrent dans le domaine de la vie privée. Comme cela a été montré, même si certains auteurs ont pu définir la vie privée comme un « ensemble d'informations personnelles », laissant ainsi supposer un chevauchement entre ces deux notions, le recouvrement n'est pas parfait[2229]. Comme l'a remarqué Madame Delphine Chauvet, il convient plutôt de retenir que « vie privée » et « données à caractère personnel » sont des notions coordonnées, mais non superposées[2230]. Ainsi, de multiples données à caractère personnel sont exclues de la notion de vie privée. Pour ces données, seule une action fondée sur l'article 82 du règlement européen est donc envisageable pour la victime.

561. L'unification des recours relatifs aux atteintes aux informations personnelles. La dualité des régimes de responsabilité fondée sur l'article 9 du code civil et sur l'article 82 du règlement européen porte atteinte à l'accessibilité et à la lisibilité du droit. En créant une fragmentation inopportune, elle rend inutilement complexes les actions en défense d'informations relatives aux personnes. Comme le soulignait Monsieur Jean-Christophe Saint-Pau, « la personnalité est une, les droits de la personnalité doivent donc tendre vers l'unité »[2231]. C'est pourquoi l'ensemble des

---

[2228] V. *supra,* n° 557.
[2229] V. *supra,* n^{os} 203 s. V. aussi, D. Gutmann, *Le sentiment d'identité. Étude de droit des personnes et de la famille*, th. Paris II, 2000, LGDJ, n° 262, p. 229 s. ; J.-C. Saint-Pau, « L'article 9 du code civil : matrice des droits de la personnalité », *D.* 1999, p. 541.
[2230] D. Chauvet, *La vie privée. Étude de droit privé,* th. Paris-Sud, 2014, n° 140, p. 123.
[2231] J.-C. Saint-Pau, « L'article 9 du code civil : matrice des droits de la personnalité », *D.* 1999, p. 541.

atteintes aux informations personnelles devraient être mises en œuvre sur un régime unifié, ou du moins cohérent.

Dans un souci de faveur pour la victime, et pour combler le déséquilibre informationnel inhérent aux traitements de données personnelles, le régime de responsabilité pour atteinte aux données personnelles doit être rapproché de celui de l'article 9 du code civil[2232]. Cette proposition s'inscrit dans la lignée jurisprudentielle reconnaissant à de très nombreuses informations personnelles (telles que la voix, l'image, l'adresse d'une personne[2233]) les bénéfices probatoires de l'article 9 du code civil.

562. L'affirmation d'une présomption simple de faute en droit des données personnelles. Pour harmoniser la mise en œuvre de ces deux droits dont l'objectif commun est de protéger les informations liées aux personnes, il est possible d'envisager un allégement du fardeau de la preuve au profit de la victime. Ainsi, une présomption simple de faute semble devoir être établie à l'égard des organismes traitant des données personnelles. De telles présomptions existent dans d'autres matières, notamment en matière contractuelle avec des obligations de moyen renforcées[2234], ou en droit médical[2235].

Plusieurs auteurs ont considéré que l'article 82 du règlement européen avait d'ores et déjà opéré une telle inversion de la charge de la preuve de la faute à l'égard de l'organisme[2236]. En effet, puisque l'article 24 du règlement européen impose aux responsables du traitement d'être en capacité de démontrer la conformité de leurs traitements aux règles du droit des données personnelles, il instaurerait *de facto* un tel inversement de la charge de la preuve. Ainsi, la victime n'aurait plus à apporter la preuve de la violation puisqu'il reviendrait au responsable du traitement de prouver son respect des règles.

[2232] Sur l'interprétation d'ores et déjà très accueillante de l'article 9 du code civil, v. A. Lepage, « L'article 9 du code civil peut-il constituer durablement la "matrice" des droits de la personnalité ? », *Gaz. Pal.* 2007, nº 139, p. 43.
[2233] V. *supra*, nos 206 s.
[2234] Cass. com., 7 avr. 2010, nº 09-12.486, *NPB*.
[2235] V. par ex. art. L. 1111-2 du code de la santé publique qui prévoit dans son huitième alinéa 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 ».
[2236] V. not. A. Danis-Fatôme, « Quelles actions judiciaires en cas de violation du RGPD ? », *CCE* 2018, nº 4, dossier 18, § 8.

Cette interprétation, bien que séduisante, doit toutefois être nuancée. En effet, si le considérant 82 du règlement européen, en lien avec l'article 24 de ce texte, énonce l'obligation pour le responsable du traitement et le sous-traitant de tenir une documentation dans l'objectif de démontrer leur conformité au droit des données personnelles, la mise à disposition de ces registres apparaît circonscrite au bénéfice des autorités de contrôle[2237]. En effet, nulle mention n'est faite quant à une éventuelle obligation pour les organismes de coopérer avec les juges. Par ailleurs, ni l'article 82 du règlement européen[2238] ni son considérant 146 ne font référence à un tel inversement de la charge de la preuve dans le cadre de l'action en responsabilité. Seul le paragraphe second de l'article 5 du règlement européen semble poser cet inversement de la charge de la preuve puisqu'il prévoit que « le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté ». Cet inversement de la charge de la preuve est donc cantonné aux principes généraux exposés dans le paragraphe premier de ce texte, c'est-à-dire aux principes de transparence, de pertinence, de minimisation des données, d'exactitude, de conservation limitée, d'intégrité et de confidentialité.

Le champ d'application de cet inversement de la preuve est réduit puisqu'il n'implique pas la démonstration de la conformité à l'ensemble des obligations prévues par ce texte, notamment celles relatives aux droits des personnes.

Pour éviter que des doutes subsistent, l'inversion du fardeau de la preuve au profit des victimes doit être juridiquement entérinée. Cette inversion se justifie aisément. D'une part, elle s'inscrit dans la dynamique actuelle du droit des données personnelles, laquelle prévoit qu'en échange de l'abandon des formalités déclaratives, les organismes sont tenus de documenter leur conformité. La documentation est donc d'ores et déjà un élément existant et n'est pas une charge supplémentaire pour l'organisme. D'autre part, cette présomption simple de faute serait une avancée pour l'unification du régime de protection des informations relatives aux personnes. Elle permettrait d'aligner le régime de protection des données personnelles sur celui du droit au respect de la vie privée.

[2237] Le considérant 82 du règlement UE nº 2016/679 dispose que « afin de démontrer qu'il respecte le présent règlement, le responsable du traitement ou le sous-traitant devrait tenir des registres pour les activités de traitement relevant de sa responsabilité. Chaque responsable du traitement et sous-traitant devrait être tenu de coopérer avec l'autorité de contrôle et de mettre ces registres à la disposition de celle-ci, sur demande, pour qu'ils servent au contrôle des opérations de traitement ».

[2238] L'article 82 du règlement UE nº 2016/679 est lié au droit à réparation et à la responsabilité.

En plus de ce renversement de la charge de la preuve, la création d'une nomenclature dans cette matière contribuerait à faciliter les actions en responsabilité.

B. La création d'une nomenclature des préjudices

563. La proposition de nomenclature. Face au faible contentieux lié aux manquements résultant d'obligations du droit des données personnelles, il semble que ce domaine pourrait bénéficier d'une approche plus méthodique. Il faut espérer qu'une meilleure détermination des contours des préjudices indemnisés encouragera les victimes à agir en défense de leurs droits et, par ricochet, garantira une meilleure application du droit des données à caractère personnel. Dans cet objectif, une proposition de nomenclature doit être formulée.

564. Plan. L'exposé des principes (1) précèdera la présentation de leur application (2).

1. Principes

565. Définitions. Si les notions de nomenclature, de barème et de référentiel sont parfois utilisées comme des synonymes, elles ont des sens différents. La nomenclature peut être définie comme une « classification méthodique des éléments d'un ensemble »[2239]. Le barème est la technique faisant correspondre une valeur monétaire à un dommage[2240]. L'utilisation d'un référentiel procède *a priori* d'une démarche différente puisqu'il s'agit d'une base ou d'un système de référence[2241]. Grâce à la publication de fourchettes d'évaluation reposant sur des données statistiques, le juge a une référence objective d'indemnisation du dommage[2242].

566. Un faux obstacle : l'interdiction des barèmes et référentiels en droit français ? En théorie, plusieurs principes du droit français s'opposent à la création de barèmes ou de référentiels. D'une part, l'interdiction des arrêts de règlement édictée par l'article 5 du code civil empêche les juges du fond de faire expressément référence

---

[2239] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vo* « Nomenclature ».
[2240] Y. Lambert-Faivre (dir.), « L'indemnisation du dommage corporel. Rapport au Garde des Sceaux », 22 juill. 2003, p. 8.
[2241] G. Cornu (dir.), *Vocabulaire juridique*, 13e éd., PUF, 2020, *Vo* « Référentiel ».
[2242] S. Porcher-Simon, « L'utilisation des barèmes en droit du dommage corporel », in *Le droit mis en barème ?,* dir. I. Sayn, Dalloz, 2014, p. 201 s., spéc. p. 202 s.

à ces barèmes dans leurs décisions[2243]. D'autre part, le principe de réparation intégrale, constamment rappelé par la Cour de cassation[2244], appelle les juges à une très grande prudence dans l'utilisation de ces outils. En effet, puisque ce principe a pour objectif de replacer la victime dans l'état dans lequel elle se serait trouvée en l'absence de l'acte dommageable, la réparation doit être parfaitement adaptée à la victime et à son dommage. Cet impératif d'adaptation *in concreto* entre en contradiction apparente avec l'utilisation d'un référentiel puisque, selon certains auteurs, il risque de s'immiscer entre le juge et le cas qui lui est soumis[2245]. En effet, les référentiels pourrait priver les juges « de leur indispensable appréciation humaine du dommage en ce qu'en faisant rentrer le cas "dans des cases", ils mécaniseraient l'indemnisation et lui feraient perdre son individualisation »[2246]. Pourtant, et comme le souligne Monsieur Clément Cousin, rien ne prouve que les juges n'utilisent pas ces référentiels au service d'une appréciation subjective[2247]. Par ailleurs, ces référentiels présentent aussi l'avantage de donner aux victimes une appréciable sécurité juridique, commandée par un objectif d'égalité, puisqu'ils harmonisent les indemnités allouées d'une juridiction à l'autre, tout en laissant une certaine souplesse aux juges[2248]. Monsieur Philippe Brun abondait dans ce sens en affirmant être « attaché à l'idée d'individualisation de la réparation (et, partant, hostile à toute forme de barèmes impératifs), et conscient que les magistrats et autres régleurs ont besoin de repères en matière d'évaluation. Toute la difficulté est d'arriver à organiser une information d'ordre statistique offrant des données chiffrées, sans dériver vers un système de forfaits rampants »[2249]. Pour résumer, tant que les référentiels laissent une souplesse suffisante aux juges, ils sont des outils utiles pour

---

[2243] L'article 5 du code civil prévoit que « Il est défendu aux juges de prononcer par voie de disposition générale et réglementaire sur les causes qui leur sont soumises ». Si, de fait, les juges du fond s'inspirent de ces barèmes, ils ne doivent pas le dire officiellement pour ne pas risquer la censure de leurs décisions par la Cour de cassation, v. not., Cass. crim., 3 nov. 1955, *D.* 1956, p. 557 ; Cass. Civ. 2e, 27 janv. 1965, nº 18-18.922, *Bull. civ.* 1965, nº 78 ; Cass. crim. 4 févr. 1970, nº 68-93.464, *Bull. crim.* 1970, nº 49, p. 115. Pour des rappels plus récents de cette solution, v. not. Cass. civ. 2e, 7 avr. 2011, nº 10-15.918, *Bull. civ.* 2010, II, nº 89 ; Cass. civ. 2e, 22 nov. 2012, nº 11-25.988, *NPB*.

[2244] Ce principe a été posé dans un arrêt de la 2e chambre civile de la Cour de cassation, v. Cass. civ. 2e, 28 oct. 1954, *JCP* 1955, p. 8765 ;

[2245] J.-B. Prévost, « Aspects philosophiques de la réparation intégrale », *Gaz. Pal* 2010, nº 100, p. 7. Pour une discussion sur la prétendue contrariété des barèmes aux principes de responsabilité civile, v. S. Porcher-Simon, « L'utilisation des barèmes en droit du dommage corporel », in *Le droit mis en barème ?,* dir. I. Sayn, Dalloz, 2014, p. 201 s., spéc. p. 204 s.

[2246] C. Cousin, « Le débat sur le référentiel indicatif de l'indemnisation du préjudice corporel des cours d'appel à l'heure des bases de données », *JCP G* 2017, nº 17, p. 483, § 7. Sur la difficulté de trouver un équilibre entre individualisation et standardisation, v. O. Leclerc, « Introduction », in *Le droit mis en barème ?,* dir. I. Sayn, Dalloz, 2014, nos 2 s., p. 115 s.

[2247] C. Cousin, « Le débat sur le référentiel indicatif de l'indemnisation du préjudice corporel des cours d'appel à l'heure des bases de données », *JCP G* 2017, nº 17, p. 483, § 7.

[2248] B. Mornet, « Pour un référentiel national d'indemnisation du dommage corporel », *Gaz. Pal.* 2010, nº 153, p. 8.

[2249] P. Brun, « De la relativité des outils d'évaluation », *Gaz. Pal.* 2012, nº 315, p. 31.

les victimes, pour les juges ainsi que pour les acteurs de l'indemnisation. Les nomenclatures présentent encore moins de risque. C'est ce qui explique qu'elles se diffusent, notamment en droit du dommage corporel.

567. Les barèmes et nomenclatures existants en matière de dommage corporel. Depuis le début des années 2000, les travaux en rapport avec l'édiction de nomenclatures et de barèmes se sont multipliés[2250]. Deux nomenclatures ont trouvé un écho particulièrement important en droit français. Leur étude apparaît nécessaire pour poser les bases d'une nomenclature dédiée aux préjudices résultant de manquements au droit des données à caractère personnel.

La première émane du groupe présidé par Madame Yvonne Lambert-Faivre[2251], et la seconde est issue du groupe dirigé par Jean-Pierre Dintilhac[2252]. Très proches l'une de l'autre, ces nomenclatures se fondent sur une triple classification commune :

(1) entre les victimes directes et les victimes indirectes,

(2) entre les préjudices patrimoniaux et les préjudices extrapatrimoniaux,

(3) et enfin, entre les préjudices temporaires antérieurs à la consolidation et les préjudices permanents postérieurs à la consolidation[2253].

Ces nomenclatures présentent également deux autres éléments importants : d'une part, elles consacrent une typologie détaillée des différents chefs de préjudice, et d'autre part, elles sont des instruments souples et ouverts, s'adaptant aux besoins du juge[2254]. Il est aujourd'hui incontestable que ces nomenclatures font partie du droit positif et ont servi de base à l'élaboration de barèmes et référentiels sur lesquels les juridictions se fondent pour évaluer les préjudices[2255]. D'ailleurs, sur la base de la

---

[2250] Si le premier barème médico-légal est apparu en 1897, de nombreux autres barèmes ont prospéré depuis. Par exemple, le barème d'invalidité des pensions militaires de 1915, le barème d'invalidité pour les accidents du travail instauré par la loi du 30 octobre 1946, le barème du concours médical publié depuis 1959, la mission d'expertise médicale adressée aux juridictions de première instance et d'appel prévue par la circulaire du 19 avril 1972, ainsi que les barèmes des fonds de garantie. Sur une brève histoire et l'évolution de ces barèmes, v. not. C. Piedelièvre, « Barèmes médicaux-légaux et missions d'expertise : évolutions », *Gaz. Pal.* 2012, nº 315, p. 17.

[2251] Y. Lambert-Faivre (dir.), « L'indemnisation du dommage corporel. Rapport au Garde des Sceaux », 22 juill. 2003.

[2252] La « nomenclature Dintilhac », du nom de l'ancien président de la deuxième chambre civile de la Cour de cassation, sous l'égide duquel fut élaborée en 2005 une nomenclature des préjudices corporels, notamment pour lutter contre les effets néfastes des barèmes locaux, v. J.-P. Dintilhac (dir.), « Rapport du groupe de travail chargé d'élaborer une nomenclature des préjudices corporels », juill. 2005.

[2253] O. Gout, « La nomenclature Dintilhac », *Gaz. Pal.* 2011, nº 358, p. 9.

[2254] O. Gout, « L'émergence de nomenclatures relatives au dommage corporel », in *Le droit mis en barème ?,* dir. I. Sayn, Dalloz, 2014, p. 227 s., spéc. p. 232.

[2255] V. not. ENM, « Référentiel indicatif de l'indemnisation du préjudice corporel des cours d'appel », sept. 2016. C. Cousin, « Le débat sur le référentiel indicatif de l'indemnisation du préjudice corporel des cours d'appel à l'heure des bases de données », *JCP G* 2017, nº 17, p. 483, § 2.

nomenclature Dintilhac, le ministère de la Justice poursuit la modélisation de l'indemnisation des dommages corporels. En effet, le décret du 27 mars 2020 organise le recensement des « montants demandés et offerts par les parties, les évaluations proposées dans le cadre de procédures de règlement amiable des litiges et les montants alloués aux victimes pour chaque type de préjudice »[2256]. Si une partie des acteurs du dommage corporel et de la doctrine restent fermement hostiles à toute « barémisation » de ce dommage[2257], un consensus s'est tout de même dégagé quant à la pertinence des nomenclatures et à leur utilité[2258].

568. Les difficultés liées à l'établissement d'une nomenclature en matière d'atteinte aux données personnelles. C'est souvent l'étude de la jurisprudence qui permet de poser les bases d'une nomenclature. Le très faible nombre d'affaires liées à la réparation de préjudices résultant d'atteinte à la protection des données à caractère personnel rend absurde l'établissement d'une nomenclature fondée uniquement sur cette jurisprudence. En revanche, la jurisprudence développée, depuis le début du XX^{e} siècle, en matière de préjudices résultant d'atteintes au droit au respect de la vie privée est très riche[2259]. Elle peut donc servir à dresser les bases d'une nomenclature en matière d'atteinte aux données personnelles. En effet, ces droits couvrent des formes d'atteinte aux personnes similaires, et l'étude des postes de préjudices dégagés par cette jurisprudence peut, à cet égard, être particulièrement utile[2260].

569. L'indemnisation des préjudices en matière d'atteinte au droit à la vie privée. Après avoir analysé plusieurs centaines de décisions de première instance et d'appel relatives à la réparation des atteintes fondées sur l'article 9 alinéa premier du

---

[2256] Décret n° 2020-356 du 27 mars 2020 portant création d'un traitement automatisé de données à caractère personnel dénommé « DataJust », *JORF* 29 mars 2020, n° 0077, texte 2. Ce décret a été critiqué par de nombreux avocats qui y voient l'avènement d'une justice algorithmique, favorisant la disparition de leur profession, v. not. C. Bernfeld, « Décret sur le traitement de données sensibles en dommage corporel sorti pendant le confinement », *anadavi.com* 2 avr. 2020 ; G. Marraud des Grottes, « Algorithme d'État : un décret lance DataJust, instrument de modélisation de l'indemnisation des dommages corporels », *Wolters Kluwer* 30 mars 2020. Pour une analyse de ce projet, A. Bensamoun et T. Douville, « Datajust, une contribution à la transformation numérique de la justice », *JCP G* 2020, n° 19, p. 582.

[2257] V. not. S. Porchy-Simon et Y. Lambert-Faivre, *Droit du dommage corporel*, 8^{e} éd., Dalloz, 2015, n° 37, p. 27 ; A. Boyer, « Référentiel d'indemnisation : des mines anti-personnel. Discours sur la méthode », *Gaz. Pal.* 2010, n° 222, p. 5.

[2258] O. Gout, « L'émergence de nomenclatures relatives au dommage corporel », in *Le droit mis en barème ?,* dir. I. Sayn, Dalloz, 2014, p. 227 s., spéc. p. 235.

[2259] Pour une analyse détaillée des éléments pris en compte par la jurisprudence dans la réparation des atteintes aux droits de la personnalité, v. C. Piccio, « La réparation de l'atteinte aux droits de la personnalité », *Légipresse* 2010, n° 273, p. 74.

[2260] Sur les liens dans la jurisprudence entre le droit au respect du droit à la vie privée et la protection des données à caractère personnel, v. *supra,* n^{os} 206 s.

code civil, quelques considérations d'ordre général peuvent être formulées[2261]. Tout d'abord, la majorité de ce contentieux est liée à la contestation, par des célébrités, d'une publication d'un article dans la presse, souvent accompagné de photographies. Ensuite, et sans surprise, aucune des décisions analysées ne reprend la distinction élaborée par les nomenclatures des dommages corporels entre les préjudices temporaires antérieurs à la consolidation et les préjudices permanents postérieurs à la consolidation, laquelle se transpose difficilement aux atteintes à la vie privée[2262].

Par ailleurs, la plupart des décisions analysées indemnise le préjudice moral de manière forfaitaire et ne distingue pas, au sein de celui-ci, les différents postes. Cette indemnisation oscille entre l'euro symbolique[2263] et quelques milliers d'euros[2264]. Dans de rares cas, l'indemnisation s'élève à plusieurs dizaines de milliers d'euros. Lorsque les juges déterminent le montant de cette réparation, ils prennent souvent en considération la place de l'article dans le journal (l'atteinte semble plus importante lorsque l'article est en couverture[2265]), la diffusion de celui-ci et l'étendue de son lectorat[2266]. Les juges prennent également en compte la nature de l'information diffusée et le comportement antérieur de la victime[2267]. Enfin, il est important de souligner que la plupart des décisions analysées n'ont pas accueilli favorablement les demandes d'indemnisation des préjudices patrimoniaux[2268].

570. Méthode retenue pour l'identification et la classification des catégories de préjudices extrapatrimoniaux indemnisés sur le fondement de l'article 9 du code

[2261] Nous avons lu et analysé près de 300 décisions rendues par les juridictions de première instance et d'appel. À ce titre, nous tenons à remercier Monsieur Antoine Dusséaux qui nous a offert un accès au site doctrine.fr. Nous avons rassemblé certaines citations des décisions les plus pertinentes dans un tableau présenté en annexe, v. Annexe 3 – Sélection de décisions de première instance et d'appel.

[2262] Certaines décisions font notamment référence aux « semaines ayant suivi la parution de l'article », v. par ex. TGI Nanterre, 1re ch., 15 mai 2008, nº 07/10721.

[2263] Principalement lorsque la preuve de l'étendue du préjudice n'est pas apportée par la victime.

[2264] La Cour européenne des droits de l'homme veille à ce que l'indemnisation soit adaptée aux faits de chaque espèce, v. CEDH, 13 juill. 1995, *Tolstoy Miloslavsky* c. *Royaume-Uni,* nº 18139/91, § 41.

[2265] V. par exemple, TGI Paris, 17e ch., 9 juill. 2008, nº 07/13908 ; TGI Paris, 17e ch., 12 nov. 2008, nº 08/03068.

[2266] V. par exemple, TGI Nanterre, 1re ch., 8 avr. 2010, nº 09/10123 ; TGI Nanterre, 1re ch., 19 janv. 2012, nº 22/03759 ; TGI Nanterre, 1re ch., 8 avr. 2010, nº 09/10123. Pour Monsieur Alain Bénabent, certains juges évaluent les dommages et intérêts au regard du bénéfice perçu par la société de presse, v. A. Bénabent, « Rapport français », in *Travaux de l'Association Henri Capitant*, « Les nouveaux moyens de reproduction (papier, sonores, audiovisuels et informatiques) », t. 37, Journées néerlandaises, Economica, 1986, p. 100.

[2267] V. par exemple, TGI Paris, 17e ch., 13 avr. 2005, nº 04/07464 ; CA Versailles, 1re ch., 27 avr. 2006, nº 05/04149.

[2268] La plupart des décisions rejettent ces demandes en les considérant comme non établies, v. not. TGI Paris, 17e ch., 24 nov. 2003, nº 02/09853. Le jugement écarte la demande en réparation de « l'énorme trouble au sein de l'entreprise et de la clientèle causé par les révélations sur la santé de son employé » ; TGI Paris, 17e ch., 13 avr. 2005, nº 04/07464, le jugement rejette la demande en réparation du préjudice professionnel ; TGI Nanterre, 1re ch., 27 mars 2007, nº 07/01131, le jugement écarte la demande en indemnisation fondée sur le fait que les publications auraient freinées les carrières des victimes ; TGI Lyon, 9e ch., 17 mai 2017, nº 14/06349, le jugement rejette la demande fondée sur le risque d'une perte d'emploi engendré par l'atteinte au droit à l'image.

civil. Si la plupart des décisions ne distinguent pas, au sein du préjudice moral, les différents chefs de préjudices indemnisés, certains jugements détaillent tout de même les atteintes prises en considération pour déterminer la réparation allouée. Ainsi, au sein du dommage moral, quatre catégories de préjudices émergent de l'étude de ces décisions.

La méthode retenue pour faire émerger ces catégories a été fondée sur une approche empirique. D'abord, la lecture des décisions a permis d'identifier, au sein de chaque décision, les préjudices pris en compte par les juges. Ensuite, les préjudices ont été organisés selon leur proximité entre eux. Par exemple, les sentiments d'anxiété, de douleur, de rumination sont assez proches et ont donc été classés au sein d'une même famille de préjudice. Enfin, un terme suffisamment générique a été attribué pour chaque famille de préjudice en fonction des types de préjudices présents. Bien sûr, comme dans la plupart des tentatives de classification, ces catégories ne sont pas immuables et devront évoluer de concert avec la jurisprudence. Néanmoins, elles sont utiles pour les personnes impliquées dans les actions en responsabilité.

571. Exposé des catégories. La première catégorie est liée au *préjudice émotionnel*, c'est-à-dire le préjudice lié aux sentiments ressentis par la victime à la suite de l'atteinte à sa vie privée. Dans cette catégorie, les juges prennent en compte les émotions ressenties par les victimes telles que l'anxiété[2269], la douleur[2270], la tristesse[2271] ou encore la honte[2272].

La deuxième catégorie de préjudice est liée au *préjudice d'exposition*, c'est-à-dire les sentiments ressentis par la victime suite à l'atteinte. Il s'agit notamment de la perte de la qualité de vie et les troubles dans les conditions d'existence que la victime subit[2273]. Les juges analysent ici les effets de l'atteinte sur la vie de la victime,

---

[2269] V. par ex. TGI Paris, 17e ch., 4 juin 2007, nº 06/15541 ; TGI Nanterre, 1re ch., 15 mai 2008, nº 07/10721 ; TGI Paris, réf., 24 nov. 2014, nº 14/59928

[2270] V. par ex. TGI Nanterre, 1re ch., 1er mars 2004, nº 03/00644 ; TGI Aix-en-Provence, réf., 25 avr. 2006, nº 06/00464 ; TGI Toulouse, 4e ch., 13 nov. 2012, nº 12/02021.

[2271] V. par ex. TGI Nanterre, 1re ch., 15 mai 2008, nº 07/10721. Sur le préjudice d'affection, v. M. Dupré, « De la souffrance à l'affection », *Gaz. Pal.* 2019, nº 15, p. 16.

[2272] V. par ex. CA Aix-en-Provence, 1re ch., 12 juin 2014, nº 13/20737 ; TGI Nanterre, 1re ch., 24 nov. 2016, nº 16/10353.

[2273] Ce poste de préjudice peut engendrer quelques difficultés lors de l'établissement du lien de causalité. En effet, pour cette catégorie de préjudice, ce sont les suites causées par l'atteinte qui sont indemnisées et non pas le préjudice immédiatement causé par l'atteinte. La Cour de cassation retient une conception de plus en plus souple du lien de causalité en matière de dommage moral, v. par ex. Cass. crim., 26 févr. 2020, nº 19-82.119, *Bull. crim.* 2020.

notamment sur sa vie affective et sociale[2274], sur sa tranquillité[2275] ou sur son anonymat[2276].

La troisième catégorie de préjudice est liée au *préjudice de pistage*, c'est-à-dire le sentiment d'être suivi, épié et soumis à une traque extérieure. Les juges s'intéressent ici aux sentiments d'impuissance[2277], de dépossession[2278] et d'acharnement[2279] subis par les victimes. En plus de ces sentiments, les juges relèvent parfois le sentiment de traque[2280], de harcèlement[2281], ou celui de se sentir sous surveillance[2282].

Enfin, la quatrième catégorie de préjudice est celle liée au *préjudice réputationnel* subi par la victime. Les juges reconnaissent ici les atteintes à la dignité[2283], à l'honneur[2284], à la réputation[2285], mais aussi le fait d'être blessé d'avoir été présenté au public d'une certaine façon[2286].

Ces quatre catégories de préjudices contribuent à l'évaluation des dommages alloués aux victimes d'atteinte au droit au respect de la vie privée et se transposent relativement bien aux atteintes résultant d'un manquement au droit des données personnelles.

2. Application

572. Les préjudices résultant d'un manquement au droit des données personnelles. Les préjudices résultant d'un manquement au droit des données personnelles n'échappent pas à la *summa divisio* traditionnelle distinguant les préjudices patrimoniaux et les préjudices extrapatrimoniaux. Comme pour les autres atteintes aux droits de la personnalité, les dommages résultant des manquements au droit des données personnelles engendrent principalement des préjudices

---

[2274] V. par ex. TGI Marseille, 1re ch., 2 juin 2009, nº 07/11509.
[2275] V. par ex. TGI Nanterre, réf., 22 sept. 2006, nº 06/01949 ; TGI Paris, 17e ch., 12 nov. 2008, nº 08/03068 ; TGI Paris, 17e ch., 7 sept. 2011, nº 10/13204.
[2276] V. par ex. TGI Nanterre, 1re ch., 1 mars 2004, nº 03/00644 ; TGI Paris, 17e ch., 2 nov.2005, nº 04/16614 ; TGI Nanterre, réf., 12 mars 2010, nº 10/00482.
[2277] V. par ex. TGI Nanterre, réf., 18 sept. 2006, nº 06/02105 ; TGI Nanterre, 1re ch., 5 mai 2011, nº 10/10082 ; TGI Nanterre, réf., 13 déc. 2016, nº 16/02457.
[2278] V. par ex. TGI Paris, réf., 14 sept. 2010, nº 10/57095 ; TGI Nanterre, 1re ch., 24 nov. 2011, nº 10/13341.
[2279] V. par ex. TGI Paris, 17e ch., 6 avr. 2005, nº 04/05663 ; TGI Nanterre, 1re ch., 8 avr. 2010, nº 09/10123.
[2280] V. par ex. TGI Paris, 17e ch., 6 avr. 2005, nº 04/05663 ; TGI Nanterre, 1re ch., 26 oct. 2006, nº 06/06902 ; TGI Nanterre, 1re ch., 19 janv. 2012, nº 11/03759.
[2281] V. par ex. TGI Paris, 17e ch., 30 mai 2007, nº 05/17887 ; TGI Paris, réf., 14 sept. 2010, nº 10/57095 ; TGI Nanterre, 1re ch., 19 mai 2011, nº 10/11475.
[2282] V. par ex. TGI Nanterre, réf., 27 janv. 2006, nº 06/00086 ; TGI Paris, 17e ch., 7 sept. 2011, nº 10/13204.
[2283] V. par ex. CA Versailles, 14e ch., 13 mai 2009, nº 09/01682 ; TGI Lyon, 9e ch., 17 mai 2017, nº 14/06349.
[2284] V. par ex. TGI Bobigny, 5e ch., 20 nov. 2018.
[2285] V. par ex. CA Rennes, 1re ch., 20 mars 2012, nº 10/04614.
[2286] V. par ex. TGI Nanterre, 1re ch., 16 janv. 2002, nº 01/03883.

extrapatrimoniaux, mais peuvent parfois résulter dans certains préjudices patrimoniaux[2287].

573. Les préjudices patrimoniaux résultant d'un manquement au droit des données personnelles. Avant d'étudier les types de préjudices patrimoniaux résultant des manquements au droit des données personnelles, il convient de rappeler que la nécessité d'élaborer une nomenclature pour ces préjudices est moins criante[2288]. Si ce besoin est avéré en droit du dommage corporel, notamment du fait des recours des tiers payeurs, un tel besoin n'est pas aussi marqué en droit des données à caractère personnel. Par ailleurs, le risque d'une nomenclature pour ces postes de préjudice est que celle-ci soit trop restrictive et qu'elle ne s'adapte pas suffisamment aux situations particulières. Enfin, les difficultés d'identification et d'évaluation de ces préjudices sont bien moins présentes que pour les préjudices extrapatrimoniaux, notamment parce qu'ils sont plus facilement évaluables en argent.

Pour autant, trois catégories de préjudices patrimoniaux peuvent être identifiées, sachant que ces catégories ne doivent pas être considérées comme exhaustives ou figées.

Tout d'abord, certains manquements au droit des données personnelles génèrent une *perte de gains professionnels*. Par exemple, un employé est licencié à la suite d'une divulgation illicite de ses données personnelles et perd ainsi ses revenus professionnels[2289].

Par ailleurs, les atteintes à la confidentialité des données engendrent souvent des *dépenses non consenties ou illicites*. Par exemple, en cas de violation fautive de données personnelles, les données subtilisées sont souvent utilisées pour effectuer ce type de dépenses. Si le code monétaire et financier organise un régime de responsabilité

[2287] Dans sa thèse sur les données personnelles, Madame Éloïse Gratton organise les dommages selon les activités de traitement effectuées sur les données. Les types de dommages résultant de ces traitements peuvent être subjectifs (sentiment d'être sous surveillance, d'humiliation, d'embarras) ou objectifs (discrimination, financier, corporel), v. É. Gratton, *Redefining personal information in the context of the Internet*, th. Paris II et Montréal, 2012, p. 247. Dans un article dédié à l'intimité sexuelle, Madame Danielle Citron présente plusieurs types de dommages vécus par les victimes de ces atteintes, notamment la peur continue que quelqu'un soit en train de les observer ou de les enregistrer, D. Citron, « Sexual privacy », *The Yale Law Journal* 2019, vol. 128, p. 1874 s. [128 YALE L.J. 1874], spéc. p. 1924.

[2288] Comme le remarquent Madame Alexandra Bensamoun et Monsieur Thibault Douville, « l'objectivité des préjudices patrimoniaux limite les difficultés liées à leur évaluation », A. Bensamoun et T. Douville, « Datajust, une contribution à la transformation numérique de la justice », *JCP G* 2020, nº 19, p. 582.

[2289] En juillet 2015, le site de rencontres extraconjugales Ashley Madison a fait l'objet d'une attaque informatique. En août 2015, suite au refus de l'entreprise de céder aux demandes des auteurs du piratage, les données de 36 millions de comptes ont été rendues publiques. Après cette publication, plusieurs utilisateurs ont déclaré avoir été licenciés par leur employeur, v. notamment T. Lamont, « Life after the Ashley Madison affair », *The Guardian* 28 févr. 2016.

en cas d'opérations de paiement non autorisées[2290], toutes les dépenses engendrées par ces violations ne sont pas nécessairement couvertes par ses dispositions. En effet, le régime de responsabilité prévu est uniquement applicable aux dépenses effectuées avec de la monnaie scripturale, et il n'existe pas de dispositions similaires pour les dépenses effectuées avec de la monnaie électronique. Il est donc parfaitement envisageable que des utilisateurs de services en ligne, ayant de la monnaie électronique ou des « jetons »[2291], ne puissent pas prétendre au remboursement, sur le fondement du code monétaire et financier, des sommes indûment dépensées. De plus, il n'est pas certain que l'article L. 133-18 du code monétaire et financier couvre l'ensemble des dépenses ayant pu être engendrées du fait de cette violation[2292]. Par exemple, si l'utilisateur a été à découvert (et que la banque lui a prélevé des agios), ou s'il subit des intérêts de retard, faute de fonds sur son compte bancaire, il n'est pas certain que les dispositions du code monétaire et financier s'appliquent également pour ces sommes indûment versées. Dès lors que les conditions de responsabilité sont établies à l'encontre d'un responsable du traitement, il n'existe aucune raison faisant barrière au remboursement de ces sommes par celui-ci.

Enfin, les atteintes aux données personnelles peuvent également engendrer certaines *dépenses de santé*, notamment un suivi psychologique pour faire face aux conséquences liées à l'atteinte subie par la personne concernée. En effet, les conséquences psychologiques d'atteinte à la protection des données personnelles peuvent être importantes.

C'est surtout à l'égard des préjudices extrapatrimoniaux que la nomenclature révèle toute son utilité.

574. Les préjudices extrapatrimoniaux résultant d'un manquement au droit des données personnelles. Les quatre catégories de préjudices extrapatrimoniaux identifiées pour les atteintes au droit au respect de la vie privée[2293] sont parfaitement

---

[2290] L'article L. 133-18 du code monétaire et financier prévoit que « En cas d'opération de paiement non autorisée signalée par l'utilisateur (…), le prestataire de services de paiement du payeur rembourse immédiatement au payeur le montant de l'opération non autorisée ». Pour une analyse de ces dispositions, v. S. Torck, « L'exécution et la contestation des opérations de paiement », *JCP E* 2010, nº 2, p. 1033.

[2291] Cela serait le cas sur un site de jeux en ligne dans lequel est échangée de la monnaie contre des jetons.

[2292] Art. L. 133-18 du code monétaire et financier. Toutefois, une interprétation de cet article pourrait laisser penser que certaines dépenses engendrées par l'opération non autorisée doivent être remboursées. En effet, cet article prévoit que, le cas échéant, le prestataire « rétablit le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu ». Pour autant, aucune jurisprudence ne confirme une telle interprétation.

[2293] V. *supra,* nº 571.

transposables au droit des données personnelles. En effet, le préjudice émotionnel, le préjudice d'exposition, le préjudice de pistage ainsi que le préjudice réputationnel sont des catégories qui se retrouvent également chez les victimes de manquements au droit des données personnelles. L'ensemble des chefs de préjudice compris dans ces catégories doivent donc être indemnisables et figurent dans la nomenclature des préjudices extrapatrimoniaux proposée[2294].

575. Le faible intérêt de la distinction des préjudices avant ou après consolidation en matière de données personnelles. En matière de préjudice résultant d'une atteinte aux droits de la personnalité, la distinction entre les préjudices temporaires antérieurs à la consolidation et les préjudices permanents postérieurs à la consolidation s'applique difficilement. En effet, contrairement aux atteintes résultant en des dommages corporels, les atteintes aux droits de la personnalité n'ont pas vraiment de « date de consolidation », c'est-à-dire qu'elles n'ont pas un « moment où les lésions se fixent et prennent un caractère permanent, tel qu'un traitement n'est plus nécessaire, si ce n'est pour éviter une aggravation »[2295]. Parfois, la consolidation coïncide avec la cessation de l'atteinte. Par exemple, si une personne usurpe le compte d'un utilisateur d'un réseau social, lorsque la victime de l'usurpation retrouve l'usage de son compte, son préjudice est alors consolidé. Ici, la fin de l'atteinte (usurpation du compte) coïncide avec la consolidation du préjudice (récupération du compte). D'autres fois, la cessation de l'atteinte ne prend jamais un caractère certain et la consolidation n'est donc pas possible. Dans les cas de violation de données par exemple, les données continuent de circuler et peuvent être réutilisées de nombreuses années après le moment de la violation[2296]. Dans ces situations, ces atteintes ont plutôt tendance à engendrer des préjudices permanents, ayant parfois un caractère évolutif.

576. L'intérêt de la reconnaissance des préjudices évolutifs en matière de données personnelles. Le préjudice moral lié aux pathologies évolutives indemnise les troubles subis par la victime en raison de la connaissance du caractère évolutif de la

[2294] V. Annexe 4 – Nomenclature des préjudices extrapatrimoniaux.
[2295] S. Porchy-Simon et Y. Lambert-Faivre, *Droit du dommage corporel*, 8e éd., Dalloz, 2015, no 84, p. 86.
[2296] Cinq années après la fuite des données du site Ashley Madison, des tentatives d'arnaque et d'extorsion perdurent encore, v. par ex. K. Fazzini, « Ashely Madison cyber-breach : 5 years later, users are being targeted with "sextorsion" scams », *CNBC* 31 janv. 2020.

pathologie dont elle est atteinte[2297]. Ce poste de préjudice, apparu récemment, indemnise les préjudices causés par des maladies incurables susceptibles d'évoluer, telles que le VIH, l'hépatite C, la maladie de Creutzfeldt-Jacob ou les maladies causées par l'amiante[2298]. Il existe en dehors de toute consolidation des blessures parce que le risque d'évolution se présente avant et après la maladie[2299].

Les manquements au droit des données à caractère personnel sont susceptibles de produire des préjudices qui s'étalent dans le temps. Par exemple, si l'image intime d'une personne est divulguée sans son consentement, celle-ci aura de grandes difficultés pour en obtenir un effacement définitif d'Internet[2300]. L'image pourra venir la hanter de nombreuses années après et lui causer de nouveaux préjudices[2301]. Les violations de données sont également susceptibles de générer une réutilisation frauduleuse des informations plusieurs années après leur survenance. Par exemple, lorsque les données récupérées illicitement sont des empreintes digitales ou de l'ADN, le risque peut se réaliser plusieurs années après. Ainsi, certains manquements au droit des données personnelles engendrent des préjudices évolutifs. Dans certains cas, la victime peut subir une aggravation de son préjudice postérieurement à la décision statuant sur l'indemnisation et elle devrait donc pouvoir saisir le juge.

577. La nécessaire prise en compte de l'éventuelle aggravation du préjudice. Par principe, tous les dommages peuvent évoluer de manière imprévisible[2302]. C'est pourquoi les mécanismes de responsabilité civile et administrative ouvrent la possibilité aux victimes d'introduire une nouvelle demande d'indemnisation en cas

---

[2297] *Rép. resp.* Dalloz, *V°* « Préjudice réparable », par F. Séners et F. Roussel, 2019 (actu. 2020), n° 290.
[2298] J.-P. Dintilhac (dir.), « Rapport du groupe de travail chargé d'élaborer une nomenclature des préjudices corporels », juill. 2005, p. 41.
[2299] *Rép. civ.* Dalloz, *V°* « Dommages et intérêts », par P. Casson, 2017 (actu. 2020), n° 79.
[2300] V. par ex. la difficulté pour les victimes d'actes pédocriminels de faire supprimer le contenu diffusé sur Internet, M. Keller et G. dance, « The Internet is overrun with images of child sexual abuse. What went wrong ? », *The New York Times* 29 sept. 2019. Plusieurs autres affaires montrent les difficultés liées à l'effacement de contenu sur Internet. Par exemple, en 2010, une institutrice avait obtenu la suppression des liens du moteur de recherche Google pointant vers une vidéo amateur à caractère pornographique la mettant en scène, TGI Montpellier, réf., 28 oct. 2010, n° 10/31735 et son appel, CA Montpellier, 5e ch., 29 sept. 2011, n° 11/00832. Autre exemple, l'affaire Max Mosley, du nom de l'ancien président de la Fédération internationale de l'automobile, à savoir la diffusion des images extraites d'une vidéo captée à son insu dans un lieu privé, le représentant dans des scènes sadomasochistes en compagnie de cinq prostituées, TGI Paris, 17e ch., 6 nov. 2013, n° 11/07970.
[2301] Pour un exemple de révélation du passé intime d'une personne, v. l'affaire *Melvin* c. *Reid* de 1931 dans laquelle une ancienne prostituée soupçonnée puis acquittée d'un meurtre avait reconstruit une nouvelle vie et s'était mariée. Huit années après ce nouveau départ, son histoire avait été révélée dans un film, *The Red Kimono*. La victime de cette révélation engagea avec succès une action contre le producteur du film, v. cour d'appel de Californie, 28 févr. 1931, *Melvin* c. *Reid*, 112 Cal. App. 285.
[2302] *Rép. resp.* Dalloz, *V°* « Hôpitaux : régimes de responsabilité et de solidarité », par C. Grossholz, 2018 (actu. 2020), n° 42.

d'aggravation du dommage[2303]. Le droit des données à caractère personnel doit également ouvrir une telle possibilité aux victimes afin de garantir une indemnisation intégrale du préjudice. Ainsi, si une aggravation du dommage apparaît postérieurement à la décision statuant sur les préjudices, la victime d'un manquement au droit des données à caractère personnel devrait pouvoir en demander réparation.

578. La question des victimes par ricochet. Certains manquements aux obligations résultant du droit des données à caractère peuvent engendrer des préjudices pour des victimes indirectes. Plusieurs situations sont à envisager. D'une part, les données peuvent être relatives à plusieurs personnes[2304]. C'est notamment le cas de l'ADN qui permet de renseigner non seulement sur la personne ayant fourni son ADN, mais également sur toute la lignée familiale. D'autre part, les manquements peuvent résulter dans des préjudices propres à certaines victimes indirectes. Par exemple, à l'occasion de la violation de données du site Ashley Madison[2305], l'épouse du mari infidèle a subi des préjudices personnels résultant des manquements de la société à son obligation de sécurité des données. Les victimes par ricochet devraient donc, elles aussi, pouvoir agir en cas de manquement.

579. L'éventuelle reconnaissance d'un préjudice collectif en matière de données personnelles. Certaines violations du droit des données personnelles causent un dommage plus étendu qu'une atteinte individuelle ou un préjudice de masse[2306]. Parfois, ces violations créent un préjudice collectif[2307]. Faute de définition, ce préjudice se comprend d'abord *a contrario* : il se distingue du préjudice subi par une association à titre individuel, et des préjudices individuels subis par un grand nombre de personnes[2308]. Le préjudice collectif peut alors être défini comme une atteinte aux

---

[2303] C. Bloch, *Droit de la responsabilité et des contrats*, Dalloz Action, 2018-2019, n° 6214.182 ; *Rép. resp.* Dalloz, *V°* « Hôpitaux : régimes de responsabilité et de solidarité », par C. Grossholz, 2018 (actu. 2020), n° 42.
[2304] V. *supra,* n° 102.
[2305] Suite à une attaque informatique, les données de 36 millions de comptes du site Ashley Madison ont été rendues publiques, v. not. T. Lamont, « Life after the Ashley Madison affair », *The Guardian* 28 févr. 2016.
[2306] Le préjudice de masse est ici entendu comme « la situation dans laquelle plusieurs personnes physiques ou morales prétendent avoir subi un préjudice à l'origine d'une perte en raison d'une même activité illicite », *Rép. proc. civ.* Dalloz, *V°* « Action de groupe », par S. Ben Hadj Yahia, 2015 (actu. 2019), n° 48.
[2307] Pour un plaidoyer sur le besoin de reconnaître un préjudice collectif en matière de données à caractère personnel, v. M. Tisné, « The data delusion : protecting individual data isn't enough when the harm is collective », 2020.
[2308] Sur ces distinctions, v. L. Boré, *La défense des intérêts collectifs par les associations devant les juridictions administratives et judiciaires*, th. Paris I, 1997, LGDJ, n° 14, p. 14. V. aussi G. Marty et P. Raynaud, *Droit civil. Les obligations*, t. 1, vol. II, Sirey, 1991, n° 385, qui considèrent que le « préjudice collectif est celui qui atteint un grand nombre d'individus… sans que l'on puisse dire que tel ou tel est particulièrement lésé ».

intérêts collectifs de l'être humain, transcendant l'intérêt individuel de chacun[2309]. Ainsi, au-delà des répercussions spécifiquement individuelles du dommage, il y a des conséquences dommageables diffuses pour des personnes non identifiées[2310]. Ce type de préjudice se développe particulièrement en droit de l'environnement[2311].

Une reconnaissance de ces préjudices en matière de données personnelles semble opportune. Par exemple, n'est-ce pas un tel préjudice qui est caractérisé en cas de manipulations résultant de traitements massifs de données personnelles[2312] ? L'entreprise Cambridge Analytica n'aurait-elle pas causé un préjudice collectif en influençant, par l'utilisation illicite de données personnelles, le vote relatif au Brexit[2313] ou l'élection de Donald Trump en 2016[2314] ? Le fait que des entreprises (telles que Facebook ou Google) autorisent la publicité ciblée (et notamment la publicité politique) a d'importantes conséquences en matière de liberté d'autodétermination et d'autonomie individuelle. Dès lors que ces publicités influencent certains utilisateurs pour obtenir un résultat politique, ne porteraient-elles pas atteinte à la collectivité dans son entier ? Il pourrait être intéressant pour certaines associations de former de tels recours afin de voir reconnaître un préjudice collectif en matière de données à caractère personnel[2315]. L'une des propositions formulées dans la présente étude d'ouvrir plus largement la capacité d'ester en justice trouve ici toute sa place[2316].

580. Conclusion de chapitre. Le droit des données personnelles prévoit de nombreuses voies de recours pour garantir le respect de ses dispositions. Leur éclatement a des conséquences négatives pour les personnes concernées, notamment parce qu'il complexifie inutilement la mise en œuvre de la protection. Cette dispersion porte atteinte à la compréhension du rôle de chaque acteur et nuit à l'interprétation

---

[2309] G. Viney, « L'action d'intérêt collectif et le droit de l'environnement écologique et sa réparation. Rapport français », in *Les responsabilités environnementales dans l'espace européen,* dir. B. Dubuisson et G. Viney, Bruylant, 2006, p. 223. V. aussi, C. Dreveau, « Réflexions sur le préjudice collectif », *RTD civ.* 2011, p. 249.
[2310] *Rép. civ.* Dalloz, *V°* « Responsabilité civile environnementale », par M. Hautereau-Boutonnet, 2019 (actu. 2020), n° 162.
[2311] Les dommages réparés sur ce chef de préjudice sont hétéroclites : ils sont d'ordre écologique, consumériste, social, économique, v. C. Dreveau, « Réflexions sur le préjudice collectif », *RTD civ.* 2011, p. 249.
[2312] Sur ces préjudices, v. *supra*, n° 456.
[2313] S. Delesalle-Stolper, « Sans Cambridge Analytica, il n'y aurait pas eu de Brexit, Interview de Christopher Wylie », *Libération* 26 mars 2018.
[2314] M. Rosenberg, N. Confessore et C. Cadwalladr, « How Trump consultants exploited the Facebook data of millions », *The New York Times* 17 mars 2018.
[2315] D'autant que la jurisprudence s'est affranchie de certaines conditions de recevabilité de l'action, notamment la nécessité de l'association d'être habilitée, v. Cass. civ. 3e, 26 sept. 2007, n° 04-20.636, *Bull. civ.* 2007, III, n° 155 ; v. aussi Cass. civ. 1re, 18 sept. 2008, n° 06-22.038, *Bull. civ.* 2008, I, n° 201.
[2316] Sur le rôle des associations et des mobilisations citoyennes en matière d'environnement, v. J. Rochfeld, *Justice pour le climat ! Les nouvelles formes de mobilisation citoyenne*, Odile Jacob, 2019, p. 75 s. et p. 149 s.

consistante du droit des données personnelles. Puisque l'article 66 de la Constitution reconnaît à l'autorité judiciaire la garde des libertés individuelles, il convient de recentrer autour de celle-ci les recours en matière de données personnelles. Par ailleurs, dès lors qu'il est fréquent que les manquements au droit des données à caractère personnel résultent dans des atteintes similaires pour de nombreuses personnes, les actions collectives doivent être encouragées. Cela passe par un assouplissement des règles liées à la capacité à agir, ainsi que par le renforcement de la coopération internationale. L'ensemble de ces mesures visent à encourager les personnes à introduire des recours et à garantir une meilleure protection de leurs données.

À ces propositions s'ajoute également le besoin de simplifier la réparation des atteintes causées par des manquements au droit des données personnelles. Cette simplification est d'autant plus nécessaire que d'importantes difficultés de preuve sont à déplorer. Pour atténuer ces difficultés et faciliter la réparation, il convient d'entériner la reconnaissance d'une présomption simple de faute à la charge des organismes traitant des données. Puisqu'ils doivent documenter leur conformité, il leur revient de rapporter la preuve de celle-ci devant un juge.

Enfin, et pour mieux indemniser les atteintes à la protection des données personnelles, les juges et les acteurs de la réparation seront invités à s'inspirer d'une nomenclature détaillant plusieurs postes de préjudices indemnisables.

581. Conclusion de titre. Pour améliorer la mise en œuvre du droit des données à caractère personnel, tous les acteurs de la matière doivent être mobilisés. Les acteurs spécialisés, tels que les autorités de contrôle, les délégués à la protection des données ou les spécialistes des données, ont une mission primordiale et historique. Ils assurent le respect des principes *via* des contrôles internes et externes.

Depuis sa création, la CNIL a vu ses missions et pouvoirs constamment augmenter. Pour autant, ses garanties d'indépendance et de procédure n'ont pas été adaptées au même rythme. Il convient donc d'actualiser les garanties d'impartialité au sein des services de la CNIL afin d'éviter des conflits d'intérêts, et il faut renforcer les garanties procédurales devant l'institution. À ces mesures s'ajoute également une revalorisation des contrôles internes à l'organisme afin de s'assurer que les spécialistes des données soient mieux responsabilisés. Ces derniers définissent souvent les modalités d'exécution des traitements de données, et ils sont donc essentiels pour garantir l'effectivité de la protection des personnes. Enfin, les coopérations

institutionnelles et avec la société civile doivent être encouragées dès lors qu'elles permettent de mutualiser des moyens et des compétences au service de la protection des personnes.

Quant aux acteurs de droit commun, l'entrée en application du règlement européen leur a octroyé une place renouvelée. Ils peuvent désormais être saisis dans le cadre de nombreuses actions (individuelles ou collectives), et il est donc possible d'espérer voir une augmentation du contentieux juridictionnel. Pour autant, la variété des voies de recours nuit à la cohérence d'ensemble de la matière, et il convient d'aiguiller ce contentieux vers le juge judiciaire, garant constitutionnel de la liberté individuelle. Pour encourager ces actions en responsabilité, il faut favoriser les actions collectives et simplifier le régime de l'action.

CONCLUSION DE LA SECONDE PARTIE

582. Le droit des données à caractère personnel doit maintenir un équilibre entre plusieurs objectifs qui apparaissent parfois contradictoires. D'un côté, il vise à protéger les personnes contre les atteintes résultant des traitements de leurs données. De l'autre, il permet aux responsables du traitement de mettre en œuvre ces traitements, notamment pour répondre aux impératifs d'une société toujours plus numérisée. Réconcilier ces deux approches est l'une des principales difficultés de ce domaine.

Souvent affichée comme la priorité du droit des données à caractère personnel, la protection des personnes peine à être pleinement effective. La pratique montre une réalité contrastée. Les six conditions permettant de justifier un traitement de données reposent sur des intérêts variés puisque seuls deux d'entre eux sont liés à la volonté de la personne. Leur articulation se révèle difficile, et des responsables du traitement ont contourné les conditions strictes d'obtention du consentement en se fondant sur la condition du contrat. Pour éviter ces stratégies de contournement, il convient d'acter la reconnaissance d'un contrat spécial de traitement de données à caractère personnel.

Par ailleurs, il est apparu que les atteintes aux personnes résultant des traitements de données prennent de nouvelles formes, et la liberté d'autodétermination se trouve ébranlée. Pour minimiser ces risques, les règles de protection ont été renforcées. Cela s'est matérialisé par un encadrement du droit à l'oubli qui permet d'éviter les risques liés à une censure privée et à la prépondérance d'intérêts individuels par rapport à ceux de la société. De plus, les transferts de données à des tiers se sont révélés porter atteinte à la protection des personnes. Des restrictions ont donc été proposées concernant ces accès. En outre, plusieurs principes importants pour garantir la liberté d'autodétermination ont dû être consolidés. Il s'agit du principe de minimisation qui évite une collecte trop large de données, et des principes entourant les prises de décision automatisées.

À l'étude, il est également apparu que le renforcement des contrôles sur les traitements de données était indispensable pour garantir une meilleure effectivité de la protection des personnes[2317]. À ce jour, l'équilibre recherché par le législateur ne peut être atteint tant que les manquements aux règles du droit des données personnelles

[2317] V. *supra,* n° 463.

continuent d'être répandus. Pour mettre fin à ces manquements, ou au moins les diminuer, tous les acteurs doivent être mobilisés.

Une telle mobilisation requiert, à l'évidence, le concours des acteurs spécialisés, bien renseignés sur les règles juridiques composant cette matière complexe. Grâce aux contrôles internes et externes qu'ils pratiquent, ils concourent indéniablement au meilleur respect de la protection des personnes. Au rôle d'aiguilleur confié à ces acteurs spécialisés, se greffe l'implacable besoin de replacer le juge judiciaire au cœur de ce contentieux. Parce qu'il bénéficie d'importantes garanties d'impartialité et d'indépendance, le gardien constitutionnel de la liberté individuelle doit retrouver en droit des données personnelles une place qu'il n'aurait jamais dû perdre[2318].

Enfin, une amélioration de la réalisation juridictionnelle a été proposée. Plus que jamais, les personnes doivent se saisir des protections juridiques pour défendre leurs droits, au risque sinon de se voir disparaître derrière le masque de leurs données. Pour les accompagner dans ces actions, des réformes procédurales ont été formulées. Tout d'abord, un élargissement de la qualité à agir des groupements pouvant introduire des recours collectifs laisse espérer leur plus grande mise en œuvre. Ensuite, la simplification du régime de l'action en responsabilité par la consécration d'une présomption simple de faute facilite cette action. Enfin, et pour mieux accompagner les personnes dans leurs actions en responsabilité, une nomenclature des préjudices a été proposée. L'ensemble de ces mesures visent à consolider l'effectivité de la protection des personnes.

[2318] Sur l'importance de l'impartialité pour la mise en œuvre effective des droits de l'homme, v. not. P. Muzny, « À quand une véritable culture des droits de l'homme en France ? », *JCP G* 2011, nº 38, p. 981.

CONCLUSION GÉNÉRALE

583. Rappel de l'objectif de l'étude et de la démarche. Le présent travail a été l'occasion de sonder l'effectivité de la protection des personnes qui résulte du droit des données à caractère personnel. En raison de l'ampleur de la matière, cette perspective s'est révélée précieuse puisqu'elle a permis d'analyser la réalité de ce droit à la lumière d'un objectif déterminé. Les conclusions de l'étude peuvent être succinctement reprises à travers l'étude de la mesure de l'effectivité de la protection des personnes par le droit des données à caractère personnel (§ I), avant de faire de brèves observations sur son importance (§ II).

§ I. La mesure de l'effectivité de la protection des personnes par le droit des données à caractère personnel

584. Des intuitions. À l'aube de cette étude, quelques questionnements et intuitions avaient été brièvement exposés. Il avait semblé que l'augmentation des traces laissées par les personnes et captées par les organismes était inhérente à la société de données. Cette société de données a amplement modifié les risques pesant sur la protection des personnes. Aujourd'hui, les traitements de données à caractère personnel ne sont plus seulement effectués pour mieux connaître les personnes, mais cherchent aussi à les influencer. Dès lors, il a été nécessaire d'étudier la façon dont le droit répond concrètement à ces risques. Il est vrai que, comme le remarquait le doyen Carbonnier, « le droit ne s'accomplit jamais exactement comme on aurait pu le prédire »[2319], et qu'en dépit des meilleures intentions, des effets négatifs pour la protection des personnes étaient à prévoir.

À première vue, le droit des données à caractère personnel sert la protection des personnes. Les principes fondateurs de la matière ont réussi à traverser les décennies sans modification profonde. En dépit de l'enthousiasme initial, des analyses

[2319] J. Carbonnier, « En l'année 1817 », *Mélanges P. Raynaud*, Dalloz, 1985, p. 81 s., spéc. p. 89.

approfondies ont mis en lumière un système plus nuancé et ont montré des besoins d'adaptation.

585. Le domaine. Le mouvement qui anime le domaine des données à caractère personnel est rythmé par les cadences de l'évolution des technologies. Fondée sur trois composantes, la notion de donnée à caractère personnel est une *donnée* qui se *rapporte* à une *personne physique*. Ces trois termes se sont révélés particulièrement larges, ce qui a permis aux acteurs de la protection des données de retenir une conception accueillante de la notion de donnée à caractère personnel. Cette tendance a été justifiée par le besoin de protéger les personnes dans toutes leurs dimensions, et cela même lorsque les données les concernant étaient très indirectement identifiantes. Des agents de la CNIL ont été par exemple jusqu'à affirmer qu'un arbre pouvait être une donnée à caractère personnel[2320] !

En apparence, un tel mouvement rassure. Cette évolution évite des stratégies de contournement et protège la personne quelles que soient les technologies de réidentification utilisées. Passé cette première impression, il est apparu qu'à terme, la notion de donnée à caractère personnel risque d'être le réceptacle de toutes les données, et que le droit positif est impuissant pour circonscrire effectivement la notion. Cet encadrement est pourtant primordial pour éviter que la protection des données à caractère personnel ne soit diluée dans un vaste ensemble de données dont les liens avec la personne existent uniquement *in abstracto*. Surtout, il s'agit d'éviter que la règlementation entrave la circulation de données qui sont trop éloignées des personnes. À cet égard, l'expansion de la notion s'est révélée avoir des effets négatifs sur les libertés individuelles. Ce sont particulièrement les libertés d'information et d'expression qui sont touchées par ces excès de qualification. Finalement, l'expansion n'atteint pas l'objectif de protection des personnes qu'elle se fixait. Au contraire, elle a même des effets pervers, souvent sous-estimés, pour la sauvegarde des autres libertés individuelles.

586. L'encadrement du domaine. Pour éviter que la notion n'accueille toutes les données pouvant se rapporter à une personne, un critère d'encadrement a été identifié. L'approche proposée s'inspire des travaux doctrinaux antérieurs et s'inscrit dans la

[2320] V. *supra,* n° 149.

notion actuelle de donnée à caractère personnel. Elle reprend la dualité classique distinguant les données directement identifiantes des données indirectement identifiantes. Seule cette dernière catégorie de données requiert un encadrement puisque, pour les données directement identifiantes, le rapport avec la personne est intrinsèque à la donnée. En effet, la fonction de ces données est précisément l'identification. Entrent donc incontestablement dans la notion les données qui relèvent de l'état des personnes telles que le nom, la date, l'heure et le lieu de naissance, l'image numérisée du visage, les empreintes digitales… En revanche, pour les données indirectement identifiantes, l'identification de la personne ne se fait qu'après un traitement particulier sur la donnée effectué par un responsable du traitement. Par exemple, pour qu'une adresse IP se rapporte à une personne, il faut croiser cette adresse IP avec d'autres données. Le critère du traitement est donc essentiel dans l'opération de qualification des données indirectement identifiantes. C'est pourquoi une approche téléologique, c'est-à-dire liée aux traitements effectués sur la donnée, s'est imposée.

Ainsi, une donnée indirectement identifiante reçoit la qualification de donnée à caractère personnel lorsque *le traitement effectué sur la donnée a pour objet ou pour effet d'établir un lien avec une personne physique*. Cette approche circonscrit le domaine de la donnée à caractère personnel puisque, lorsque la donnée est indirectement identifiante, seuls les traitements rattachant la donnée à la personne déclenchent la qualification. Un tel critère présente deux bénéfices. D'une part, il garantit la protection des données liées aux personnes en s'assurant que toutes les données qui s'y rapportent entrent dans la notion de données à caractère personnel. D'autre part, il permet aux données trop éloignées des personnes de circuler librement, contribuant ainsi aux libertés d'information et d'expression.

Cette nouvelle définition a commandé un renforcement du régime de protection des données à caractère personnel.

587. L'amélioration des règles. Le régime déclaratif, décrié pour son manque d'efficacité, a été remplacé par un régime de responsabilité fondé sur le principe « Faites confiance, mais vérifiez »[2321]. L'étude du droit positif révèle un droit favorable

[2321] Il s'agit du proverbe russe « Доверяй, но проверяй » (Trust but verify) régulièrement utilisé par le président américain Ronald Reagan, v. Opinion, « Trust, but verify », *The New York Times* 10 déc. 1987.

à la mise en œuvre des traitements de données à caractère personnel. Cela est particulièrement patent lors de l'analyse des conditions de licéité du traitement.

Tandis que quatre fondements possibles sont basés sur un intérêt extérieur à la personne concernée, seuls deux d'entre eux lui sont directement liés. Le premier est lié au consentement de la personne concernée et le second renvoie au contrat auquel celle-ci est partie. Naturellement, des difficultés d'articulation entre ces deux conditions liées à la volonté de la personne ont vu le jour, et des responsables du traitement ont contourné les conditions strictes d'obtention du consentement en invoquant le bénéfice du fondement contractuel. Pour éviter de laisser prospérer cette entorse à la protection des personnes, la reconnaissance d'un contrat spécial de traitement de donnée à caractère personnel a été défendue. Celui-ci s'applique lorsque le contrat a pour objet le traitement de données à caractère personnel. Parce que les dispositions particulières de ce contrat permettent d'obtenir un consentement libre et éclairé pouvant être retiré à tout moment, la protection de la personne concernée se trouve alors renforcée.

Par ailleurs, les nouvelles formes d'atteintes aux personnes permises par les traitements de données personnelles peinent à être appréhendées efficacement par la règlementation actuelle. Depuis quelques années, les risques liés à la société de surveillance[2322] sont couplés à ceux attachés à la société de manipulation. Les traitements de données ne sont plus seulement passifs, c'est-à-dire destinés à surveiller les personnes, ils enrichissent des modèles prédictifs qui permettent ensuite de mieux les influencer. Touchées dans leur liberté d'autodétermination[2323], les personnes sont souvent inconscientes de ces manipulations pernicieuses. Pour répondre à ces risques, le droit des données à caractère personnel doit évoluer et certains principes doivent être adaptés.

Pour éviter que la liberté d'accéder à l'information ne dépende des compétences techniques de ses bénéficiaires, notamment en contournant les mesures de déréférencement, le droit à l'oubli récemment consacré doit être circonscrit. La possibilité de demander l'effacement de données à caractère personnel doit donc se limiter aux seules publications jugées illicites. En tout état de cause, la mise en balance entre le droit de la personne concernée à l'effacement de ses données, celui du

[2322] La surveillance est non seulement étatique mais est aussi mise en œuvre par les grandes entreprises, v. S. Zuboff, *The age of surveillance capitalism : the fight for a human future at the new frontier of power,* PublicAffairs, 2019.
[2323] Sur ce concept, v. *supra,* n^os^ 288 s.

responsable du traitement et celui du public à accéder à l'information relève de la compétence des juges et non pas de celle des moteurs de recherche.

De plus, pour renforcer la prérogative de contrôle des personnes concernées à l'égard de leurs données, ce sont les accès aux données par des tiers qui ont dû être restreints. Le droit positif est, sur ce point, trop souple, et les transmissions de données à des tiers sont trop courantes. Pour encadrer plus strictement ces transferts, il convient de les rendre plus transparents pour la personne concernée et d'obtenir son consentement exprès.

Ensuite, il a semblé impératif de consolider le principe de minimisation qui restreint les données collectées et diminue les possibilités de les croiser pour réidentifier les personnes. Cette consolidation passe par une application stricte des règles de proportionnalité et par une augmentation des contrôles.

Enfin, ce sont les règles encadrant les prises de décision automatisées qui ont été renforcées afin de prévenir les manipulations des personnes. Ce renforcement s'est traduit par une meilleure mise en œuvre, au sein des organismes traitant des données, des principes de loyauté et de vigilance.

Au cours de ces développements, un fil rouge s'est dessiné : ce ne sont pas les principes de protection qui appellent le plus grand nombre de modifications puisque de simples ajustements permettent d'améliorer nettement la protection des personnes ; renforcer l'effectivité de la protection des personnes passe surtout par une amélioration de la mise en œuvre du droit des données à caractère personnel.

588. L'amélioration de la mise en œuvre du droit des données à caractère personnel. Assurer l'effectivité de la protection des personnes passe par un renforcement des contrôles ainsi que par une amélioration de la réalisation juridictionnelle du droit des données à caractère personnel.

En premier lieu, l'amélioration des contrôles implique de réformer la CNIL. Doivent ainsi être renforcées les règles d'indépendance de ses services et les garanties procédurales devant elle. Quant à sa composition, elle doit être modifiée pour que l'institution bénéficie, en son sein, d'une meilleure représentation des experts techniques. À côté des actions de la CNIL, les contrôles internes au sein des organismes traitant des données doivent être augmentés. À ce titre, le rôle du délégué à la protection des données est important. Toutefois, ce délégué ne peut être la seule personne, au sein de l'organisme, à garantir le respect du droit des données à caractère personnel. Les

experts techniques doivent se voir reconnaître un plus grand rôle, ainsi qu'une plus grande responsabilité, notamment *via* la création d'une charte éthique, dans les choix liés aux traitements de données. Enfin, et pour épauler l'action des services de la CNIL, l'augmentation des collaborations avec des institutions et la société civile, ainsi que des coopérations internationales se sont révélées précieuses.

En second lieu, l'amélioration de la réalisation juridictionnelle passe par un recentrage des interventions des acteurs de cette matière. Devant la confusion liée à la variété des recours offerts aux personnes concernées, il a fallu canaliser, autour du juge judiciaire, le contentieux de la protection des données personnelles. Cela se justifie aisément puisque l'autorité judiciaire est, selon la Constitution, la gardienne de la liberté individuelle[2324]. C'est pourquoi l'autorité judiciaire connaît du contentieux des droits de la personnalité et du droit au respect de la vie privée. Par ailleurs, l'accès au juge pourrait être simplifié par une plus large ouverture de l'exercice des recours collectifs. Ces actions sont cruciales puisque les manquements au droit des données à caractère personnel engendrent souvent des préjudices similaires pour de nombreux usagers du service. Enfin, et pour favoriser les recours, ce sont les conditions des actions en responsabilité délictuelle qui ont été ajustées. Cela s'est matérialisé par la consécration d'une présomption simple de faute à la charge de l'organisme traitant des données, et par l'établissement d'une nomenclature des préjudices résultant des manquements au droit des données personnelles.

Plutôt qu'une opposition tranchée entre une protection effective ou ineffective des personnes, notre étude a montré que la protection des personnes par le droit des données à caractère s'apprécie selon des degrés différents[2325]. Grâce à certains ajustements, les règles améliorent l'effectivité de la protection des personnes, laquelle apparaît essentielle à l'heure où les traitements de données sont si répandus.

[2324] R. Desgorces, « Les armes du juge judiciaire dans la protection des libertés fondamentales : le point de vue de la doctrine », in *Colloque La guerre des juges aura-t-elle lieu ? Analyse comparée des offices du juge administratif et du juge judiciaire dans la protection des libertés fondamentales,* dir. G. Éveillard, 2016.
[2325] J. Carbonnier, « Effectivité et ineffectivité de la règle de droit », *L'année sociologique* 1957-1958, vol. 9, p. 3, spéc. p. 14.

§ II. L'importance du droit des données à caractère personnel pour l'effectivité de la protection des personnes

589. Des tensions géopolitiques. À la fin du XX[e] siècle, un socle normatif international commun s'est dessiné. Plusieurs instances, notamment l'OCDE, le Conseil de l'Europe et l'ONU, ont adopté des principes supranationaux relatifs à la protection des données à caractère personnel. Ces standards internationaux de protection ont favorisé le développement du commerce international et des services numériques entre les pays.

Plusieurs facteurs ont érodé la confiance mutuelle et entravé la quête d'une harmonisation des règles de protection entre les pays. L'émergence de multinationales quasi-monopolistiques a engendré une forme de défiance[2326], ou au moins une certaine jalousie, à l'égard des États-Unis. Les scandales liés aux campagnes de surveillance massive des citoyens et des représentants politiques de pays européens ont également altéré la confiance vis-à-vis de ce pays. Un principe de « défiance mutuelle » entre l'Europe et les États-Unis s'est progressivement esquissé[2327]. Les annulations successives du *Safe Harbor*[2328] et du *Privacy Shield*[2329], c'est-à-dire des mécanismes d'auto-certification permettant aux entreprises établies aux États-Unis de transférer des données collectées en Europe vers ce pays, en sont les meilleurs témoins.

D'autres grands acteurs étrangers gagnent le territoire européen. Récemment, ce sont les acteurs chinois et russes, avec des services tels que *TikTok, WeChat* ou *FaceApp,* qui bénéficient d'une popularité croissante. Ces nations ont des conceptions encore plus éloignées de la protection des personnes et de leurs libertés que celles que nous partageons entre Europe et les États-Unis[2330]. Des menaces renouvelées risquent donc de peser sur l'effectivité de la protection des personnes, et le droit devra de nouveau s'adapter pour y répondre[2331].

[2326] L'action intentée le 20 octobre 2020 par le ministère de la Justice américain en est l'un des témoins, v. B. Kendall et R. Copeland, « Justice department hits Google with antitrust lawsuit », *The Wall Street Journal* 20 oct. 2020.
[2327] B. Haftel, « Transferts transatlantiques de données personnelles : la Cour de justice invalide le *Safe Harbour* et consacre un principe de défiance mutuelle », *D.* 2016, p. 111.
[2328] CJUE, 6 oct. 2015, *Maximillian Schrems* c. *Data Protection Commissioner,* C-362/14, § 88 s.
[2329] CJUE, 16 juill. 2020, *Data Protection Commissioner* c. *Facebook Ireland Ltd, Maximillian Schrems,* C-311/18, § 168 s.
[2330] Pour un bref aperçu des atteintes aux droits de l'homme dans ces pays, v. Amnesty, « China overview », 2019 et Amnesty, « Russian Federation overview », 2019.
[2331] En opposition avec les obligations de transparence algorithmique prévues par le droit européen, la Chine a prévu qu'il n'était pas possible d'exporter librement un algorithme de recommandations personnalisées basées sur de l'analyse de données. Dès lors, ce n'est qu'après une autorisation du gouvernement chinois que cette

590. Vers une meilleure effectivité de la protection des personnes. La contribution du droit des données à caractère personnel à l'effectivité de la protection des personnes est incontestable. Il offre aux personnes concernées un contrôle sur leurs données et la possibilité de se défendre contre les manipulations. Toutefois, « le droit n'est pas cet absolu dont souvent nous rêvons »[2332] ; il est trop humain pour prétendre à l'absolu. Le droit évolue au gré de la société, des technologies et de l'air du temps[2333]. Il en est le reflet et n'oserait prétendre assurer, à lui seul, l'effectivité de la protection des personnes. Au crépuscule de ce travail, nous formulerons donc l'espoir de voir les technologies accompagner les principes juridiques pour renforcer l'effectivité de la protection des personnes.

exportation sera permise, Y. Yang et R. McMorrow, « What China's new export rules mean for TikTok's US sale », *Financial Times* 31 août 2020.

[2332] J. Carbonnier, *Flexible droit. Pour une sociologie du droit sans rigueur*, 10e éd., LGDJ, 2001, p. 487.

[2333] Le constitutionnaliste américain Paul Freund avait déclaré que « the Court should never be influenced by the weather of the day but inevitably they will be influenced by the climate of the era », pouvant être traduit par « la cour ne devrait jamais été influencée par le temps qu'il fait mais elle sera immanquablement influencée par l'air du temps ».

BIBLIOGRAPHIE

Plan de la bibliographie :

§ I. Ouvrages, traités, manuels et cours

A. Juridiques

Atias (C.), *Droit civil. Les biens,* 12e éd., Paris, LexisNexis, 2014, coll. « Manuels ».
Atias (C.), *Épistémologie juridique,* Paris, PUF, 1985, coll. « Droit fondamental ».
Aubert (J.-L.) **et Savaux** (E.), *Introduction au droit et thèmes fondamentaux du droit civil*, 18e éd., Paris, Sirey, 2020, coll. « Sirey université ».
Aubry (C.) **et Rau** (C.), *Cours de droit civil français d'après la méthode de Zachariæ,* t. 9, 5e éd., par **Bartin** (E.), Paris, Librairies techniques, 1917, disponible à : https://gallica.bnf.fr/ark:/12148/bpt6k5493942t.
Auby (J.-M.) et **Ducos-Ader** (R.), *Le droit de l'information*, Paris, Dalloz, 1982, coll. « Précis ».
Azoulai (L.), **Barbou des Places** (S.) et **Pataut** (E.) (dir.), *Constructing the person in EU law : rights, roles, identities*, Portland, Bloomsbury Publishing, 2016.
Bacache-Gibelli (M.), *La responsabilité civile extracontractuelle,* 3e éd., Paris, Economica, 2016, coll. « Corpus ».
Batiffol (H.), *Problèmes de base de philosophie du droit*, Paris, LGDJ, 1979.
Beignier (B.) et **Binet** (J.-R.), *Droit des personnes et de la famille*, 4e éd., Paris, LGDJ, 2019, coll. « Cours ».
Beignier (B.), **Lamy** (B. de) et **Dreyer** (E.) (dir.), *Traité de droit de la presse et des médias*, Paris, LexisNexis, 2009.
Bellivier (F.), *Droit des personnes*, Paris, LGDJ, 2015, coll. « Précis Domat ».
Benabou (V.-L.) et **Rochfeld** (J.), *À qui profite le clic ? Le partage de la valeur à l'ère numérique*, Paris, Odile Jacob, 2015, coll. « Corpus ».
Bergel (J.-L.), *Théorie générale du droit*, 5e éd., Paris, Dalloz, 2012.
Binctin (N.), *Droit de la propriété intellectuelle. Droit d'auteur, brevet, droits voisins, marque, dessins et modèles,* 6e éd., Paris, LGDJ, 2020, coll. « Manuel ».

Bioy (X.), *Droits fondamentaux et libertés publiques*, 5e éd., Paris, LGDJ, 2018, coll. « Cours ».
Bloch (C.), *Droit de la responsabilité et des contrats*, Paris, Dalloz, 2018-2019, coll. « Dalloz Action ».
Bouloc (B.), *Procédure pénale,* 27e éd., Paris, Dalloz, 2019, coll. « Précis ».
Bourgeois (M.), *Droit de la donnée. Principes théoriques et approche pratique,* Paris, LexisNexis, 2017, coll. « Droit & Professionnels ».
Braconnay (N.), *La justice et les institutions juridictionnelles*, 3e éd., Paris, La Documentation française, 2019.
Brun (P.), *Responsabilité civile extracontractuelle*, 5e éd., Paris, LexisNexis, 2018, coll. « Manuels ».
Buffelan-Lanore (Y.) et **Larribau-Terneyre** (V.), *Droit civil. Introduction, biens, personnes, famille,* 21e éd., Paris, Sirey, 2019, coll. « Sirey université ».
Burdon (M.), *Digital data collection and information privacy law*, Cambridge, Cambridge University Press, 2000.
Carbonnier (J.), *Droit civil, 1/ Les personnes,* 20e éd., Paris, PUF, 1996, coll. « Thémis Droit ».
Carbonnier (J.), *Droit civil,* t. 4, *Les obligations*, 22e éd., Paris, PUF, 2000, coll. « Thémis Droit ».
Carbonnier (J.), *Droit civil,* vol. 1, *Introduction. Les personnes. La famille, l'enfant, le couple*, Paris, PUF, 2004, coll. « Quadrige ».
Carbonnier (J.), *Droit civil,* vol. 2, *Les biens. Les obligations*, Paris, PUF, 2004, coll. « Quadrige ».
Carbonnier (J.), *Droit civil. 1/ Les personnes*, 21e éd., PUF, 2000, coll. « Thémis ».
Carbonnier (J.), *Droit et passion du droit sous la Ve République,* Paris, Flammarion, 1996, coll. « Essais ».
Carbonnier (J.), *Flexible droit. Pour une sociologie du droit sans rigueur*, 10e éd., Paris, LGDJ, 2001.
Caron (C.), *Droit d'auteur et droits voisins*, 5e éd., Paris, LexisNexis, 2017, coll. « Manuels ».
Cayrol (N.), *Procédure civile*, Paris, Dalloz, 2e ed., 2019, coll. « Cours ».
Chaltiel (F.), *Les lanceurs d'alerte,* Paris, Dalloz, 2018, coll. « Connaissance du droit ».
Chapus (R.), *Droit administratif général*, t. 1, 15e éd., Paris, Montchrestien, 2001, coll. « Précis Domat ».
Chemerinsky (E.), *Constitutional law: principles and policies*, 6e éd., Wolters Kluwer, 2019.
Cooley (T.), *A treatise on the law of torts or the wrongs which arise independent of contract*, vol. 1, 2e éd., Chicago, Callaghan and Company, 1888, disponible à : https://repository.law.umich.edu/books/11/.
Cooter (R.) et **Ulen** (T.), *Law and economics*, 6e éd., Addison-Wesley, 2012, disponible à : https://web.archive.org/web/20160726175150/https:/scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1001&context=books.
Cornu (G.), *Droit civil. Introduction. Les personnes. Les biens*. 11e éd., Paris, Montchrestien, 2003, coll. « Précis Domat ».
Cornu (G.), *Droit civil. Les personnes*, 13e éd., Paris, Montchrestien, 2007, coll. « Précis Domat ».
Costa (J.-P.), *La Cour européenne des droits de l'homme. Des juges pour la liberté,* 2e éd., Paris, Dalloz, 2017, coll. « Les sens du droit ».
Dabin (J.), *Le droit subjectif*, Paris, Dalloz, 1952, réimpr. 2007.
Debet (A.), **Massot** (J.) et **Métallinos** (N.), *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Paris, Lextenso, 2015, coll. « Les Intégrales ».
Dejean de la Bâtie (N.), *Droit civil français*, t. VI-2, dir. **Aubry** (C.) et **Rau** (C.), 8e éd., Paris, Litec, 1989.
Demogue (R.), *Les notions fondamentales du droit privé*, Paris, Librairie Arthur Rousseau, 1911, disponible à : https://gallica.bnf.fr/ark:/12148/bpt6k5457266z.

Demogue (R.), *Traité des obligations en général,* t. 2, Paris, Librairie Arthur Rousseau, 1923, disponible à : https://gallica.bnf.fr/ark:/12148/bpt6k6477714q.
Fabre-Magnan (M.), *Droit des obligations,* t. 1, *Contrat et engagement unilatéral*, 5e éd., Paris, PUF, 2019, coll. « Thémis ».
Fabre-Magnan (M.), *Droit des obligations,* t. 2, *Responsabilité civile et quasi-contrats*, 4e éd., Paris, PUF, 2019, coll. « Thémis ».
Fabre-Magnan (M.), *Introduction au droit,* Paris, PUF, 2018, coll. « Que sais-je ? ».
Fabre-Magnan (M.), *L'institution de la liberté*, Paris, PUF, 2018.
Fabre-Magnan (M.) et **Brunet** (F.), *Introduction générale au droit,* Paris, PUF, 2017, coll. « Thémis ».
Favoreu (L.) *et al.*, *Droit constitutionnel,* 23e éd., Paris, Dalloz, 2020, coll. « Précis ».
Favoreu (L.) *et al.*, *Droit des libertés fondamentales*, 7e éd., Paris, Dalloz, 2015, coll. « Précis ».
Féral-Schuhl (C.), *Cyberdroit 2020/2021,* 8e éd., Paris, Dalloz, 2020, coll. « Praxis Dalloz ».
Flour (J.), **Aubert** (J.-L.) et **Savaux** (E.), *Droit civil. Les obligations,* t. 2, *Le fait juridique,* 14e éd., Paris, Sirey, 2011, coll. « Sirey université ».
Flour (J.), **Aubert** (J.-L.) et **Savaux** (E.), *Les obligations,* t. 2, *Le fait juridique,* 14e éd., Paris, Sirey, 2011, coll. « Sirey université ».
Flour (J.), **Aubert** (J.-L.) et **Savaux** (E.), *Les obligations.* t. 1, *L'acte juridique,* 16e éd., Paris, Sirey, 2014, coll. « Sirey université ».
Frayssinet (J.), *Informatique fichiers et libertés,* Paris, Litec, 1992.
Fried (C.), *An anatomy of values : problems of personal and social choice*, Cambridge, Harvard University Press, 1970.
Frier (P.-L.) et **Petit** (J.), *Précis de droit administratif*, 5e éd., Paris, Montchrestien, 2008, coll. « Précis Domat ».
Gaïa (P.), **Ghevontian** (R.), **Mélin-Soucramanien** (F.), **Roux** (A.) et **Oliva** (E.), *Les grandes décisions du Conseil constitutionnel*, 19e éd., Paris, Dalloz, 2018, coll. « Grands arrêts ».
Gauthier (C.), **Platon** (S.) et **Szymczak** (D.), *Droit européen des droits de l'Homme,* Paris, Sirey, 2016, coll. « Sirey université ».
Gautier (P.-Y.), *Propriété littéraire et artistique*, 11e éd., Paris, PUF, 2019, coll. « Droit fondamental ».
Gellert (R.), *The risk-based approach to data protection*, Oxford, Oxford University Press, 2020.
Genevois (B.), *La jurisprudence du Conseil constitutionnel*, Sciences et Techniques Humaines, 1988.
Gény (F.), *Méthodes d'interprétation et sources en droit privé positif,* t. 1, Paris, LGDJ, 1919, disponible à : https://gallica.bnf.fr/ark:/12148/bpt6k3332127r.
Ghestin (J.), **Loiseau** (G.) et **Serinet** (Y.-M), *La formation du contrat*, 4e éd., 2013, coll. « Traités ».
González Fuster (G.), *The emergence of personal data protection as a fundamental right of the EU*, Springer, 2014.
Goubeaux (G.), *Traité de droit civil. Les personnes*, Paris, LGDJ, 1989.
Grimaldi (M.), *Droit des successions,* 7e éd., Paris, LexisNexis, 2017, coll. « Manuels ».
Guinchard (S.) *et al.*, *Droit processuel. Droits fondamentaux du procès*, 10e éd., Paris, Dalloz, 2019, coll. « Précis ».
Hennette-Vauchez (S.) et **Roman** (D.), *Droits de l'Homme et libertés fondamentales*, 4e éd., Paris, Dalloz, 2020, coll. « HyperCours ».
Hoofnagle (C.), *Federal Trade Commission. Privacy law and policy*, Cambridge, Cambridge University Press, 2016.
Kane (R.), *A contemporary introduction to free will,* Oxford, Oxford University Press, 2005.
Kayser (P.), *La protection de la vie privée par le droit*, 3e éd., Paris, Economica, 1995.
Kayser (P.), *La protection de la vie privée*, 2e éd., Paris, Economica, 1990.
Kelsen (H.), *La théorie pure du droit. Introduction à la science du droit*, La braconnière, 1953.
Kosta (E.), *Consent in the European data protection law*, Leiden, Leiden Nijhoff Publishers, 2013.

Kuner (C.), *European Data Protection Law : Corporate Compliance and Regulation*, 2e éd., Oxford, OUP Oxford, 2007.
Laferrière (É.), *Traité de la juridiction administrative et des recours contentieux*, t. 1, 2e éd., Paris, Berger-Levrault, 1896, disponible à : https://gallica.bnf.fr/ark:/12148/bpt6k5728025j.
Lagarde (P.) et **Loussouarn** (Y.) dir., *L'information en droit privé : travaux de la conférence d'agrégation*, Paris, LGDJ, 1978.
Lamberterie (I. de) et **Lucas** (J.-H.) (dir.), *Informatique, libertés et recherche médicale*, Paris, CNRS, 2001, coll. « Droit ».
Lane (F.), *American privacy : the 400-year history of our most contested right*, Boston, Beacon Press, 2009.
Larroumet (C.) et **Bros** (S.), *Traité de droit civil. Les obligations, le contrat*, t. 3, 9e éd., Paris, Economica, 2018, coll. « Corpus ».
Latina (M.) et **Chantepie** (G.), *Le nouveau droit des obligations*, 2e éd., Paris, Dalloz, 2018.
Lessig (L.), *The future of ideas : the fate of the commons in a connected world,* New York, Random House, 2001.
Lochak (D.), *Les droits de l'homme*, Paris, La Découverte, 2018, coll. « Repères ».
Loiseau (G.), *Le droit des personnes*, 2e éd., Paris, Ellipses, 2020.
Lucas (A.), **Devèze** (J.) et **Frayssinet** (J.), *Droit de l'informatique et de l'Internet*, Paris, PUF, 2001, coll. « Thémis ».
Lucas (A.), *Le droit de l'informatique*, Paris, PUF, 1987, coll. « Thémis ».
Lucas (A.), **Lucas-Schloetter** (A.) et **Bernault** (C.), *Traité de la propriété littéraire et artistique*, 5e éd., Paris, LexisNexis, 2017, coll. « Traités ».
Mainguy (D.), *Contrats spéciaux*, 11e éd., Paris, Dalloz, 2018, coll. « Cours ».
Malaurie (P.) et **Aynès** (L.), *Cours de droit Civil,* t. 2, *Les Personnes, les incapacités*, 5e éd., Cujas, 1999.
Malaurie (P.) et **Aynès** (L.), *Droit des personnes. La protection des mineurs et des majeurs*, 8e éd., Paris, LGDJ, 2015, coll. « Droit civil ».
Malaurie (P.), **Aynès** (L.) et **Stoffel-Munck** (P.), *Droit des obligations*, 10e éd., Paris, LGDJ, 2018, coll. « Droit civil ».
Malinvaud (P.), *Introduction à l'étude du droit*, 20e éd., Paris, LexisNexis, 2020, coll. « Manuels ».
Malinvaud (P.), **Mekki** (M.) et **Seube** (J.-B.), *Droit des obligations*, 15e éd., Paris, LexisNexis, 2019, coll. « Manuels ».
Marais (A.), *Droits des personnes*, 3e éd., Paris, Dalloz, 2018, coll. « Cours ».
Martial-Braz (N.) et **Rochfeld** (J.) (dir.), *Droit des données personnelles. Les spécificités du droit français au regard du RGPD,* Paris, Dalloz, 2019, coll. « Décryptage ».
Marty (G.) et **Raynaud** (P.), *Droit civil. Les obligations*, t. 1, vol. II, Paris, Sirey, 1991.
Mathieu (B.) et **Verpeaux** (M.) (dir.), *Transparence et vie publique. Neuvième printemps du droit constitutionnel*, Paris, Dalloz, 2015, coll. « Thèmes et commentaires ».
Mattatia (F.), *RGPD et droit des données personnelles,* 4e éd., Paris, Eyrolles, 2019.
Mazeaud (H.), **Mazeaud** (L.) et **Tunc** (A.), *Traité théorique et pratique de la responsabilité civile délictuelle et contractuelle,* t. 1, 6e éd., Paris, Montchrestien, 1965.
Mazeaud (H.), **Mazeaud** (L.), **Mazeaud** (J.) et **Chabas** (F.), *Leçons de droit civil,* t. 2, vol. I, *Obligations*, 9e éd., par **Chabas** (F.), Paris, Montchrestien, 1998.
McCarthy (T.) et **Schechter** (R.) (dir.), *The Rights of Publicity and Privacy*, 2e éd., Thomson Reuters, 2020.
Michael (J.), *Privacy and Human Rights, an international and comparative study, with special reference to developments in information technology*, Unesco, 1994.
Mill (J. S.), *De la liberté*, Paris, Gallimard, 1990, coll. « Essais ».
Miller (A.), *Assault on Privacy, Computers, Data Banks, and Dossiers*, Ann Arbor, The University of Michigan Press, 1971.
Mounier (E.), *Le personnalisme,* Paris, PUF, 2010, coll. « Quadrige ».
Mourgeon (J.), *Les droits de l'homme*, 8e éd., Paris, PUF, 2008, coll. « Que sais-je ? ».
Netter (E.), *Numérique et grandes notions du droit privé. La personne, la propriété, le contrat*, mémoire en vue de l'habilitation à diriger des recherches en droit privé, Picardie, 2017,

disponible à : https://enetter.fr/wp-content/uploads/2018/09/E.-NETTER-Nume%CC%81rique-et-grandes-notions-du-droit-prive%CC%81-V.-1.06.pdf.
Oberdorff (H.), *Droits de l'homme et libertés fondamentales,* 7e éd., Paris, LGDJ, 2019, coll. « Manuel ».
Perreau (E.-H.), *Le droit au nom en matière civile*, Paris, Sirey, 1910.
Perrot (R.), **Beignier** (B.) et **Miniato** (L.), *Institutions judiciaires*, 17e éd., Paris, LGDJ, 2018, coll. « Précis Domat ».
Planiol (M.), *Traité élémentaire de droit civil*, t. 1, 11e éd., Paris, LGDJ, 1920, disponible à : https://gallica.bnf.fr/ark:/12148/bpt6k11599814.
Planiol (M.), *Traité élémentaire de droit civil*, t. 2, 11e éd., Paris, LGDJ, 1931, disponible à : https://gallica.bnf.fr/ark:/12148/bpt6k1159982j.
Porchy-Simon (S.) et **Lambert-Faivre** (Y.), *Droit du dommage corporel*, 8e éd., Paris, Dalloz, 2015, coll. « Précis ».
Porchy-Simon (S.), *Droit civil 2e année. Les obligations,* 10e éd., Paris, Dalloz, 2017, coll. « Hypercours ».
Portalis (J.-É.-M.), *Discours préliminaire au premier projet de Code civil*, Bordeaux, Confluences, 1999, disponible à : https://mafr.fr/IMG/pdf/discours_1er_code_civil.pdf.
Poulet-Gibot Leclerc (N.), *Droit administratif : sources, moyens, contrôles*, Bréal, 2007.
Poullet (Y.), *La vie privée à l'heure de la société numérique,* Bruxelles, Larcier, 2019, coll. « Crids ».
Pousson-Petit (J.) (dir.), *L'identité de la personne humaine : étude de droit français et de droit comparé*, Bruxelles, Bruylant, 2003.
Pradel (J.), *Procédure pénale,* 20e éd., Cujas, 2019, coll. « Référence ».
Prélot (P.-H.), *Droit des libertés fondamentales*, 2e éd., Hachette Supérieur, 2010.
Rassat (M.-L.), *Traité de procédure pénale*, Paris, PUF, 2001, coll. « Droit fondamental ».
Ricard (J.), *Droit et jurisprudence en matière de postes, télégraphes, téléphones*, t. 1, Paris, Sirey, 1931, disponible à : https://gallica.bnf.fr/ark:/12148/bpt6k6313179v.
Rigaux (F.), *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Bruylant, 1990.
Ripert (G.), *Aspects juridiques du capitalisme moderne*, 2e éd., Paris, LGDJ, 1955.
Ripert (G), *La règle morale dans les obligations civiles*, 4e éd., Paris, LGDJ, 1949.
Roagna (I.), *La protection du droit au respect de la vie privée et familiale par la Convention européenne des droits de l'homme*, Conseil de l'Europe, 2012, disponible à : https://rm.coe.int/168007ff65.
Rochfeld (J.), *Justice pour le climat ! Les nouvelles formes de mobilisation citoyenne*, Paris, Odile Jacob, 2019.
Rochfeld (J.), *Les grandes notions du droit privé,* 2e éd., Paris, PUF, 2013, coll. « Thémis ».
Roubier (P.), *Le droit de la propriété industrielle*, t. 1, Paris, Sirey, 1952.
Royer-Collard (P.-P.), *De la liberté de la presse*, Paris, Librairie de Médicis, 1949, disponible à : https://gallica.bnf.fr/ark:/12148/bpt6k49969d.
Sacco (R.), *La comparaison juridique au service de la connaissance du Droit*, Paris, Economica, 1991.
Saint-Pau (J.-C.) (dir.), *Droits de la personnalité,* Paris, LexisNexis, 2013, coll. « Traités ».
Sauron (J.-L.) et **Chartrier** (A.), *Les droits protégés par la Convention européenne des droits de l'homme*, Paris, Gualino, 2014, coll. « Master ».
Savatier (R.), *Traité de la responsabilité civile en droit français,* t. 2, 2e éd., Paris, LGDJ, 1951.
Schwartz (P.) et **Solove** (D.), *Information privacy law*, 6e éd., Wolters Kluwer, 2018.
Starck (B.), **Roland** (H.) et **Boyer** (L.), *Obligations*, vol. I, *Responsabilité délictuelle*, 5e éd., Paris, Litec, 1996.
Sudre (F.) (dir.), *Droit européen et international des droits de l'homme*, 14e éd., Paris, PUF, 2019, coll. « Droit fondamental ».
Supiot (A.), *La Gouvernance par les nombres. Cours au Collège de France (2012-2014)*, Paris, Fayard, 2015, coll. « Poids et Mesures du Monde ».

Tambou (O.), *Manuel de droit européen de la protection des données à caractère personnel*, Bruxelles, Bruylant, 2020, coll. « Droit administratif ».
Terré (F.) et **Fenouillet** (D.), *Droit civil. La famille,* 8e éd., Paris, Dalloz, 2012, coll. « Précis ».
Terré (F.) et **Fenouillet** (D.), *Droit civil. Les personnes*, 8e éd., Paris, Dalloz, 2012, coll. « Précis ».
Terré (F.) et **Molfessis** (N.), *Introduction générale au droit*, 11e éd., Paris, Dalloz, 2019, coll. « Précis ».
Terré (F.) et **Simler** (P.), *Droit civil. Les biens*, 10e éd., Paris, Dalloz, 2018, coll. « Précis ».
Terré (F.), **Simler** (P.), **Lequette** (Y.) et **Chénedé** (F.), *Droit civil. Les obligations,* 12e éd., Paris, Dalloz, 2018, coll. « Précis ».
Terwangne (C. de) et **Rosier** (K.), *Le règlement général sur la protection des données. Analyse approfondie,* Larcier, 2018, coll. « Crids ».
Teyssié (B.), *Droit des personnes*, 20e éd., Paris, LexisNexis, 2018, coll. « Manuels ».
Teyssié (B.), *Droit des personnes*, 21e éd., Paris, LexisNexis, 2019, coll. « Manuels ».
Viney (G.), **Jourdain** (P.) et **Carval** (S.), *Les effets de la responsabilité,* 4e éd., Paris, LGDJ, 2017, coll. « Traités ».
Vivant (M.) et **Bruguière** (J.-M.), *Droit d'auteur et droits voisins*, 4e éd., Paris, Dalloz, 2019, coll. « Précis ».
Waline (J.), *Droit administratif,* 28e éd., Paris, Dalloz, 2020, coll. « Précis ».
Westin (A.), *Privacy and Freedom*, New York, Ig Publishing, 1968, réimpr. 2015.
Zenati (F.) et **Revet** (T.), *Les biens*, 3e éd., Paris, PUF, 2008, coll. « Droit fondamental ».
Zenati-Castaing (F.) et **Revet** (T.), *Manuel de droit des personnes*, Paris, PUF, 2006, coll. « Droit fondamental ».

B. Extra-juridiques

About (I.) **et Denis** (V.), *Histoire de l'identification des personnes*, Paris, La Découverte, 2010.
Allen (A.), *Uneasy access : privacy for women in a free society,* Totowa, Rowman & Littelfield, 1953.
Angeli (C.) **et Mesnier** (S.), *Les micros du Canard,* Paris, Les arènes, 2014.
Ariès (P.), *L'enfant et la vie familiale sous l'Ancien Régime*, Paris, Seuil, 1973.
Bentham (J.), *Panopticon or the inspection house*, vol. 1, Londres, Payne, 1791, disponible à : https://www.ics.uci.edu/~djp3/classes/2012_01_INF241/papers/PANOPTICON.pdf.
Benyayer (L.-D.) et **Chignard** (S.), *Datanomics. Les nouveaux business models des données*, Limoges, FYP, 2015.
Boudard (L.) et **Geiselhart** (D.), *Les possédés. Comment la nouvelle oligarchie de la tech a pris le contrôle de nos vies,* Paris, Arkhé, 2019.
Briet (S.), *Qu'est-ce que la documentation ?*, Paris, EDIT, 1951, disponible à : http://martinetl.free.fr/suzannebriet/questcequeladocumentation/briet.pdf.
Cardon (D.), *À quoi rêvent les algorithmes : nos vies à l'heure des big data,* Paris, Seuil, 2015.
Coulanges (F. de), *La Cité antique. Étude sur le culte, le droit, les institutions de la Grèce et de Rome,* 1866, Cambridge, Cambridge University Press, réimpr. 2009, disponible à : https://letterepaoline.files.wordpress.com/2014/02/fustel-de-coulanges-la-citc3a9-antique.pdf.
Coulmont (B.), *Sociologie des prénoms*, Paris, La Découverte, 2014, coll. « Repères ».
Cowen (Z.), *The private man*, Australian Broadcasting Commission, 1969.
Danan (Y. M.), *Histoire postale et libertés publiques*, Paris, LGDJ, 1965.
Delort (P.), *Le big data*, 2e éd., Paris, PUF, 2018, coll. « Que sais-je ? ».
Desrosières (A.), *La politique des grands nombres. Histoire de la raison statistique,* Paris, La Découverte, 2010.
Duby (G.) et **Ariès** (P.) (dir.), *Histoire de la vie privée*, t. 1 à 5, Paris, Seuil, 1999.
Eleb (M.) et **Debarre** (A.), *Architectures de la vie* privée, Paris, Hazan, 1999.

Foucault (M.), *Surveiller et punir. Naissance de la prison*, Paris, Gallimard, 1975, coll. « Tel », disponible à : https://monoskop.org/images/2/22/Foucault_Michel_Surveiller_et_Punir_Naissance_de_la_Prison_2004.pdf.
Garfinkel (S.), *Database Nation, The Death of Privacy in the 21st Century*, Sebastopol, O'Reilly, 2000.
Kotu (V.) et **Deshpande** (B.), *Data science. Concepts and practice,* 2e éd., Morgan Kaufmann, 2018.
Le Bart (C.), *L'individualisation*, Paris, Presses de Sciences Po, 2008, coll. « Références ».
Leleu-Merviel (S.), *La traque informationnelle*, ISTE Éditions, 2017.
Mény (Y.), *La corruption de la République*, Paris, Fayard, 1992.
Nissenbaum (H.), *Privacy rights in context. Technology, policy, and the integrity of social life,* Stanford, Stanford University Press, 2010.
Noiriel (G.), *L'identification. Genèse d'un travail d'État*, Paris, Belin, 2007, coll. « Socio-histoires ».
Nozick (R.), *Anarchie, État et utopie,* Paris, PUF, 1974, coll. « Quadrige ».
O'Neil (C.), *Weapons of math destruction. How big data increases inequality and threatens democracy*, New York, Crown New York, 2016.
Orwell (G.), *1984,* Paris, Gallimard, 1949, disponible à : https://www.samizdat.qc.ca/arts/lit/PDFs/1984_GO.pdf.
Otlet (P.), *Traité de documentation*, Bruxelles, Mundaneum, 1934, disponible à : https://fr.wikisource.org/wiki/Page:Otlet_-_Trait%C3%A9_de_documentation,_1934.djvu/28.
Pariser (E.), *The filter bubble,* Penguin Press, 2011.
Ricœur (P.), *Soi-même comme un autre*, Paris, Seuil, 1996.
Rifkin (J.), *La troisième révolution industrielle*, Arles, Actes sud, 2013.
Schneier (B.), *Data and Goliath : The hidden battles to collect your data and control your world*, New York, Norton & Company, 2015.
Tricot (A.), **Sahut** (G.) et **Lemarié** (J.), *Le document : communication et mémoire*, Louvain-la-Neuve, De Boeck, 2016, coll. « Information et stratégie ».
Tüfekçi (Z.), *Twitter and tear gas: the power and fragility of networked protest,* Londres, Yale University Press, 2017.
Wolf (V.), *A room of one's own,* Feedbooks, 1929, disponible à : http://seas3.elte.hu/coursematerial/PikliNatalia/Virginia_Woolf_-_A_Room_of_Ones_Own.pdf.
Zuboff (S.), *The age of surveillance capitalism : the fight for a human future at the new frontier of power,* PublicAffairs, 2019.

§ II. Thèses

Agostinelli (X.), *Le droit à l'information face à la protection civile de la vie privée*, th. Aix-en-Provence, 1994, Librairie de l'Université d'Aix-en-Provence.
Alliot (S.), *Essai de qualification de la notion de données à caractère personnel,* th. Besançon, 2018.
Allix (N.), *Les sanctions pécuniaires civiles,* th. Paris II, 2020.
Ancel (P.), *L'indisponibilité des droits de la personnalité. Une étude critique des droits de la personnalité,* th. Dijon, 1978.
Anciaux (N.), *Essai sur l'être en droit privé*, th. Paris II, 2018, LexisNexis.
Antoine (V.), *Le consentement en procédure pénale*, th. Montpellier, 2011, disponible à : https://theses.fr/2011MON10040.
Arminjon (C.), *Étude sur les droits du particulier dans son domicile et sur les restrictions que ces droits subissent dans l'intérêt public*, th. Dijon, 1900.
Audier (J.), *Les droits patrimoniaux à caractère personnel*, th. Marseille, 1979, LGDJ.

Audit (P.-E.), *La naissance des créances : approche critique du conceptualisme juridique*, th. Paris II, 2013, Dalloz.
Balat (N.), *Essai sur le droit commun*, th. Paris II, 2014, LGDJ.
Beignier (B.), *L'honneur et le droit*, th. Paris II, 1995, LGDJ.
Benzina (S.), *L'effectivité des décisions QPC du Conseil constitutionnel*, th. Paris II, 2016, LGDJ.
Bertrand-Mirkovic (A.), *La notion de personne (étude visant à clarifier le statut juridique de l'enfant à naître)*, th. Aix-Marseille, 2003, PUAM, disponible à : https://books.openedition.org/puam/1108.
Betaille (J.), *Les conditions juridiques de l'effectivité de la norme en droit public interne : illustrations en droit de l'urbanisme et en droit de l'environnement,* th. Limoges, 2012, disponible à : https://theses.fr/2012LIMO1007.
Boré (L.), *La défense des intérêts collectifs par les associations devant les autorités administratives et judiciaires*, th. Paris I, 1997, LGDJ.
Bourgeois (M.), *La personne objet de contrat*, th. Paris I, 2003, Paradigme.
Brasselet (R.), *La circulation de la donnée à caractère personnel relative à la santé*, th. Lorraine, 2018, disponible à : https://theses.fr/2018LORR0333.
Brocal von Plauen (F.), *Le droit à l'information en France*, th. Lyon II, 2004, disponible à : https://theses.univ-lyon2.fr/documents/lyon2/2004/brocal_f#p=1&a=TH.1.
Bussy-Dunan (F.), *Le concours d'action en justice entre les mêmes parties. L'étendue de la faculté de choix du plaideur,* 1987, th. Paris I, LGDJ.
Cadiet (L.), *Le préjudice d'agrément*, th. Poitiers, 1983.
Carval (S.), *La responsabilité civile dans sa fonction de peine privée,* th. Paris I, 1995, LGDJ.
Chambardon (N.), *L'identité numérique de la personne humaine : contribution à l'étude du droit fondamental à la protection des données à caractères personnel,* th. Lyon II, 2018, disponible à : https://hal.archives-ouvertes.fr/tel-02464483.
Chardeau (M.-A.), *Les choses communes*, th. Paris I, 2004, LGDJ.
Chauvet (D.), *La vie privée. Étude de droit privé,* th. Paris-Sud, 2014.
Coulibaly (I.), *La protection des données à caractère personnel dans le domaine de la recherche scientifique*, th. Grenoble, 2011, disponible à : https://tel.archives-ouvertes.fr/tel-00798112.
Cousin (C.), *Vers une redéfinition de l'acte médical*, th. Rennes I, 2016, disponible à : https://ged.univ-rennes1.fr/nuxeo/site/esupversions/5fbf6c2e-fafd-476f-86b2-4eb1956586a8?inline.
Couveinhes (F.), *L'effectivité en droit international public*, th. Paris II, 2011, disponible à : https://theses.fr/2011PA020058.
Debaets (E.), *Le droit à la protection des données à caractère personnel. Recherche sur un droit fondamental*, th. Paris I, 2014.
Debet (A.), *L'influence de la Convention européenne des droits de l'homme sur le droit civil*, th. Paris II, 2002, Dalloz.
Deschanel (C.), *Le droit patrimonial à l'image : émergence d'un nouveau droit voisin du droit d'auteur*, th. Aix-Marseille, 2017, disponible à : https://tel.archives-ouvertes.fr/tel-01753401/document.
Douville (T.), *Les conflits d'intérêts en droit privé*, th. Caen, 2013, Institut universitaire Varenne.
Drouot (G.), *La rétroactivité de la jurisprudence. Recherche sur la lutte contre l'insécurité juridique*, th. Paris II, 2014, LGDJ.
Dubois (C.), *Responsabilité civile et responsabilité pénale. À la recherche d'une cohérence perdue,* th. Paris II, 2014, LGDJ.
Dumenil (G.), *Le domicile en droit pénal,* th. Paris II, 2017.
Eynard (J.), *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon.
Eyraud (A.-F.), *Le contrat réel. Essai d'un renouveau par le droit des biens*, th. Paris I, 2003.
Fabre-Magnan (M.), *Essai d'une théorie de l'obligation d'information dans les contrats*, th. Paris I, 1992, LGDJ.

Fenouillet (D.), *La conscience*, th. Paris II, 1993, LGDJ.
Filippone (C.), *La contractualisation des droits de la personnalité,* th. Paris I, 2001.
Galbois (D.), *La notion de contrat. Esquisse d'une théorie*, th. Paris II, 2018.
Gali (H.), *Le préjudice moral en droit de la responsabilité civile,* th. Paris-Saclay, 2019.
Givord (F.), *La réparation du préjudice moral*, th. Grenoble, 1938, Dalloz.
Gratton (É.), *Redefining personal information in the context of the Internet*, th. Paris II et Montréal, 2012.
Gravelais (I.), *La protection juridictionnelle de l'inviolabilité du domicile,* th. Dijon, 2013, disponible à : https://hal-univ-bourgogne.archives-ouvertes.fr/tel-01563871/document.
Guégan-Lécuyer (A.), *Dommages de masse et responsabilité civile*, th. Paris I, 2006, LGDJ.
Gutmann (D.), *Le sentiment d'identité. Étude de droit des personnes et de la famille*, th. Paris II, 2000, LGDJ.
Henry (X.), *La technique de qualifications contractuelles,* th. Nancy II, 1992.
Houin (B.), *La rupture unilatérale des contrats synallagmatiques,* th. Paris II, 1973.
Hyde (A.-A.), *Les atteintes aux libertés individuelles par contrat. Contribution à la théorie de l'obligation,* th. Paris I, 2015, IRJS.
Iosca (B.), *L'effectivité de la sanction des infractions au code de la route,* th. Toulon, 2014.
Koumpli (C.), *Les données personnelles sensibles. Contribution à l'évolution du droit fondamental à la protection des données à caractère personnel*, th. Paris I, 2019.
Labarthe (F.), *La notion de document contractuel,* th. Paris I, 1994, LGDJ.
Lanna (M.), *La protection des données à caractère personnel à l'épreuve de l'automesure connectée*, th. Paris II, 2019.
Larouer (M.), *Les codes de conduite, sources du droit*, th. Lyon, 2016, Dalloz.
Le Clainche (J.), *L'adaptation du droit des données à caractère personnel aux communications électroniques,* th. Montpellier I, 2008.
Le Goues (M.), *Le consentement du patient en droit de la santé*, th. Perpignan, 2015, disponible à : https://tel.archives-ouvertes.fr/tel-01267019/document.
Lécuyer (G.), *Liberté d'expression et responsabilité. Étude de droit privé,* th. Paris I, 2004, Dalloz.
Lelieur-Fischer (J.), *La règle ne bis in idem : du principe de l'autorité de la chose jugée au principe d'unicité d'action répressive. Étude à la lumière des droits français, allemand et européen*, th. Paris I, 2005.
Lesaulnier (F.), *L'information nominative,* th. Paris II, 2005.
Levy (C.), *La personne humaine en droit*, th. Paris I, 2000.
Limbach (F.), *Le consentement contractuel à l'épreuve des conditions générales des contrats : de l'utilité du concept de la déclaration de volonté*, th. Toulouse I et Université de la Sarre, 2003, LGDJ.
Loiseau (G.), *Le nom, objet d'un contrat*, th. Paris I, 1995, LGDJ.
Luciani (A.-M.), *Les droits de la personnalité. Du droit interne au droit international privé*, th. Paris I, 1996.
Lumaret (C.), *L'effet horizontal de la Charte des droits fondamentaux de l'Union européenne*, th. Paris II, 2015.
Marbillard (V.), *Les effets de la transparence sur la confiance des citoyens. Clarification conceptuelle et étude de cas empire au niveau local*, th. Lausanne, 2019, disponible à : https://serval.unil.ch/resource/serval:BIB_CB3AE70B74B7.P002/REF.
Marot (P.-Y.), *Les données et informations à caractère personnel. Essai sur la notion et ses fonctions,* th. Nancy, 2007.
Masson (F.), *La propriété commune*, th. Paris I, 2016, disponible à : https://theses.fr/2016PA01D013.
Mattatia (F.), *La protection des données à caractère personnel face aux usages illicites, déloyaux et frauduleux,* th. Paris X, 2010.
Merabet (S.), *Vers un droit de l'intelligence artificielle,* th. Aix-Marseille, 2018, Dalloz.
Moron-Puech (B.), *Contrat ou acte juridique ? Étude à partir de la relation médicale*, th. Paris II, 2016, LGDJ, disponible à : https://hal.archives-ouvertes.fr/tel-01384293v4.

Motulsky (H.), *Principes d'une réalisation méthodique du droit privé. La théorie des éléments générateurs des droits subjectifs*, th. Lyon, 1948, réimpr. Dalloz, 2002.
Nerson (R.), *Les droits extrapatrimoniaux*, th. Lyon, 1939, Bosc Frères.
Ochoa (N.), *Le droit des données personnelles, une police administrative spéciale*, th. Paris I, 2014, disponible à : https://tel.archives-ouvertes.fr/tel-01340600.
Peltier (V.), *Le secret des correspondances,* th. Aix-Marseille, 1998, PUAM.
Pétel-Teyssié (I.), *Les durées d'efficacité du contrat*, th. Montpellier, 1984.
Porteau-Azoulai (S.), *Le pouvoir réglementaire de la Commission nationale de l'information et des libertés,* th. Paris II, 1993.
Porumb (O.), *La rupture des contrats à durée indéterminée par volonté unilatérale,* th. Paris, 1937.
Rabut (A.), *De la notion de faute en droit privé,* th. Paris, 1946, LGDJ.
Ravanas (J.), *La protection des personnes contre la réalisation et la publication de leur image*, th. Aix-en-Provence, 1978, LGDJ.
Rossi (J.), *Protection des données personnelles et droit à la vie privée : enquête sur la notion controversée de « donnée à caractère personnel »*, th. Compiègne, 2020, disponible à : https://www.julienrossi.com/these.pdf.
Rouhette (G.), *Contribution à l'étude critique de la notion de contrat*, th. Paris, 1965.
Rouxel (S.), *Recherches sur la distinction du dommage et du préjudice,* th. Grenoble, 1994.
Sagné (V.), *L'identité de la personne humaine,* th. Toulouse I, 2003.
Saint-Pau (J.-C.), *L'anonymat et le droit*, th. Bordeaux, 1998.
Serna (M.), *L'image et le droit*, th. Paris II, 1994, Economica.
Supiot (A.), *Le juge et le droit du travail,* th. Bordeaux I, 1979.
Terré (F.), *De l'influence de la volonté individuelle sur les qualifications*, th. Paris, 1955, LGDJ, réimpr. 2014, coll. « Anthologie du droit ».
Thullier (B.), *L'autorisation. Étude de droit privé*, th. Paris X, 1993, LGDJ.
Tricot-Chamard (I.), *Contribution à l'étude des droits de la personnalité. L'influence de la télévision sur la conception juridique de la personnalité*, th. Paris I, 2004, PUAM.
Tzutzuiano (C.), *L'effectivité de la sanction pénale*, th. Toulon, 2015, disponible à : https://tel.archives-ouvertes.fr/tel-01405168.
Van Couvering (E.), *Search engine bias. The structuration of traffic on the World-Wide Web*, th. London School of Economics and Political Science, 2009, disponible à : https://etheses.lse.ac.uk/41/1/Van_Couvering_Search_engine_bias.pdf.
Zenati (F.), *Essai sur la nature juridique de la propriété : contribution à la théorie du droit subjectif*, th. Lyon III, 1981.
Zwolinska (M.), *Sécurité et libertés fondamentales des communications électroniques en droit français, européen et international*, th. Nice, 2015, disponible à : https://tel.archives-ouvertes.fr/tel-01251984/document.

§ III. Articles, chroniques, notes, observations, mémoires, commentaires et conférences

A. Juridiques

A. (P.) et **M.** (H.) note ss. CA Paris, 15 mai 1970, *Jean Ferrat*, *D.* 1970, p. 466.
Agostini (E.), « La protection du nom patronymique et la nature du droit au nom », *D.* 1973, p. 313.
Alemanno (A.), **Helleringer** (G.) et **Sibony** (A.-L.), « Brève introduction à l'analyse comportementale du droit », *D.* 2016, p. 911.
Alleaume (C.), « Les données à caractère personnel comme objet des contrats », *AJ Contrat* 2019, p. 373.

Allen (A.), « Privacy-as-data control : conceptual, practical and moral limits of the paradigm », *Connecticut Law Review* 1999, vol. 32, p. 861, disponible à : https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1789&context=faculty_scholarship.
Altman (I.), « Privacy regulation : culturally universal of culturally specific ? », *Journal of social issues* 1977, vol. 33, p. 67, disponible à : https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1045.1753&rep=rep1&type=pdf.
Amarani-Mekki (S.), « Le socle commun procédural de l'action de groupe de la loi de modernisation de la justice du XXIe siècle. À propos de la loi no 2016-1547 du 18 novembre 2016 », *JCP G* 2016, no 50, p. 1340.
Amson (D.), « L'indemnisation du préjudice résultant des atteintes à la vie privée », *Légipresse* 2002, no 195, p. 128.
Ancel (M.-É.), « D'une diversité à l'autre. À propos de la "marge de manœuvre" laissée par le règlement général sur la protection des données aux États membres », *Revue critique de droit international privé* 2019, p. 647.
Ancel (P.), « Force obligatoire et contenu obligationnel », *RTD civ.* 1999, p. 771.
Ancel (P.), « La protection des données personnelles : aspects de droit privé français », *RID comp.* 1987, vol. 39, no 3, p. 609, disponible à : https://www.persee.fr/doc/ridc_0035-3337_1987_num_39_3_2729.
Andrieu (E.), « Internet et la protection des données personnelles », *Legicom* 2000, no 21-22, p. 155, disponible à : https://www.cairn.info/revue-legicom-2000-1-page-155.htm.
Antippas (J.) et **Beignier** (B.), « La protection de la vie privée », in *Libertés et droits fondamentaux 2020*, **Cabrillac** (R.) (dir.), 26e éd., Dalloz, 2020, p. 203.
Antippas (J.), « Propos dissidents sur les droits dits "patrimoniaux" de la personnalité », *RTD com.* 2012, p. 35.
Azar-Baud (M. J.), « (In)action de groupe », *Gaz. Pal.* 2016, no 23, p. 52.
Azzi (T.), « Les relations entre la responsabilité civile délictuelle et les droits subjectifs », *RTD civ.* 2007, p. 227, no 8.
Bacache (M.), « Action de groupe et responsabilité civile », *RTD civ.* 2014, p. 450.
Bacache (M.), « Corps humain. Têtes maories », *RTD civ.* 2010, p. 626.
Badinter (R.), « Le droit au respect de la vie privée », *JCP G* 1968, I, doctr. 2136.
Baechler (J.), « Les libertés d'opinion et d'expression », *RDP* 2015, no 2, p. 308.
Balat (N.), « Le cumul d'actions en droit des obligations », *D.* 2020, p. 1819.
Banck (A.), « GDPR et sous-traitance : un nouveau devoir de conseil ? », *Dalloz IP/IT* 2017, p. 36.
Béguin-Faynel (C.), « Héritage numérique & cadavre(s). Pour un testament des dernières volontés numériques », in *Traité des nouveaux droits de la mort*, t. 2, dir. **Touzeil-Divina** (M.), **Bouteille-Brigant** (M.) et **Boudet** (J.-F.), Lextenso, 2014, p. 67.
Beignier (B.), « Rapport Français », in *Travaux de l'Association Henri Capitant*, « La discrimination », t. 51, Journées franco-belges, SLC, 2004, p. 604.
Bénabent (A.), « Rapport français », in *Travaux de l'Association Henri Capitant*, « Les nouveaux moyens de reproduction (papier, sonores, audiovisuels et informatiques) », t. 37, Journées néerlandaises, Economica, 1986, p. 100.
Benabou (V.-L.) et **Rochfeld** (J.), « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte I : Le moteur, facilitateur d'accès, agrégateur d'informations et responsable de traitement autonome », *D.* 2014, p. 1476.
Benabou (V.-L.), « L'extension du domaine de la donnée », *Légicom* 2017, no 59, p. 3.
Bensamou (A.) et **Douville** (T.), « Datajust, une contribution à la transformation numérique de la justice », *JCP G* 2020, no 19, p. 582.
Bensamoun (A.) et **Zolynski** (C.), « *Big data* et *privacy* : comment concilier nouveaux modèles d'affaires et droits des utilisateurs ? », colloque du Forum des sciences sociales, Montréal, 15 oct. 2013, *LPA* 18 août 2014, no 164, p. 8.
Bensamoun (A.) et **Zolynski** (C.), « *Cloud computing* et *big data*. Quel encadrement pour ces nouveaux usages des données personnelles ? », *Réseaux* 2015, no 189, p. 103.

Bensamoun (A.), « Les droits fondamentaux et Internet », in *Libertés et droits fondamentaux 2020*, dir. Cabrillac (R.), 26e éd., Dalloz, 2020, p. 307.
Bensoussan (A.), « À terme, le droit de valoriser ses propres données apparaît inéluctable », *RLDI* 2018, nº 153, p. 54.
Béraud (J.-M.), « Entretien annuel d'évaluation des salariés, consultation du CHSCT et déclaration auprès de la CNIL », *Le Droit Ouvrier* 2008, p. 49, disponible à : https://ledroitouvrier.cgt.fr/IMG/pdf/200802_doctrine_beraud.pdf.
Bergé (J.-S.) et **Le Métayer** (D.), « Phénomènes de masse et droit des données », *CCE* 2018, nº 12, étude 20.
Bernard (D.), « Article 50 – Droit à ne pas être jugé ou puni pénalement deux fois pour une même infraction », in *Charte des droits fondamentaux de l'Union européenne. Commentaire article par article*, dir. **Picod** (F.) et **Van Drooghenbroeck** (S.), p. 1039.
Bernelin (M.), « La patrimonialisation des données personnelles : entre représentation(s) et réalité(s) juridiques, *JCP G* 2019, nº 46, doctr. 1172.
Bernfeld (C.), « Décret sur le traitement de données sensibles en dommage corporel sorti pendant le confinement », *anadavi.com* 2 avr. 2020, disponible à : https://anadavi.com/dotclear/index.php/post/2020/04/02/D%C3%A9cret-sur-le-traitement-de-donn%C3%A9es-sensibles-en-dommage-corporel-sorti-pendant-le-confinement.
Bernheim-Desvaux (S.), « Nouvelle donne pour les consommateurs : la directive omnibus est publiée ! », *CCC* 2020, nº 2, comm. 33.
Bernt Hugentholtz (P.), « Propriété des données », in *Mélanges M. Vivant,* Dalloz, 2020, p. 205.
Bicheron (F.), « La mort numérique », in *Mélanges M. Grimaldi*, Defrénois, 2020, p. 81.
Bioy (X.), « Le libre développement de la personnalité en droit constitutionnel, essai de comparaison Allemagne, Espagne, France, Italie, Suisse », *RID comp.* 2003, vol. 55, nº 1, p. 123, disponible à : https://www.persee.fr/doc/ridc_0035-3337_2003_num_55_1_5563.
Bîrsan (C.), « La notion de domicile au sens de l'article 8 de la Convention vise le siège social, les agences et les locaux professionnels d'une personne morale », *D.* 2003, p. 527.
Blanc (N.) et **Gautier** (P.-Y), « Contre "l'anonymisation" des arrêts publiés : décadence des références de jurisprudence », *D.* 2019, p. 1648.
Blanc-Gonnet Jonason (P.), « Vers une meilleure adaptation du droit de la protection des données personnelles à la réalité informationnelle », *AJDA* 2008, p. 2105.
Bloud-Rey (C.), « Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles », *D.* 2013, p. 2795.
Boev (I.), « Le nouveau règlement : un 5e principe de libre circulation ? », *Dalloz IP/IT* 2020, p. 223.
Boizard (M.), « Données à caractère personnel – Le consentement à l'exploitation des données à caractère personnel : une douce illusion ? », *CCE* 2016, nº 3, étude 6.
Boizard (M.), « Le temps, le droit à l'oubli et le droit à l'effacement », *Les cahiers de la justice* 2016, p. 619.
Bonneau (J.), « L'accès au dossier médical », *Gaz. Pal.* 2003, nº 127, p. 3.
Boré (L.), « Discours à la table ronde "Pour mieux réparer les préjudices collectifs : une *class action* à la française ?" », *Gaz. Pal.* 2001, nº 271, p. 4.
Boré (L.), « Le projet d'action de groupe : action mort-née ou premier pas ? », *Gaz. Pal.* 2013, nº 136, p. 29.
Boré (L.), « Les deux fonctions des juridictions suprêmes », *JCP G* 2018, nº 1-2, p. 33.
Borghetti (J.-S.), « Les intérêts protégés et l'étendue des préjudices réparables en droit de la responsabilité civile extra-contractuelle », in *Mélanges G. Viney*, LGDJ, 2008, p. 145.
Bourgeois (M.) et **Thibierge** (L.), « Droit de la donnée : plaidoyer pour un régime général », *JCP E* 2020, nº 20, p. 1207.
Boursier (M.-E.), « Qu'est-ce que la *compliance* ? Essai de définition », *D.* 2020, p. 1419.
Boy (L.), « Réflexions sur le "le droit de la régulation" », *D.* 2001, p. 3031.
Boyer (A.), « Référentiel d'indemnisation : des mines anti-personnel. Discours sur la méthode », *Gaz. Pal.* 2010, nº 222, p. 5.

Braibant (G.), « La protection des droits individuels au regard du développement de l'informatique », *RID comp.* 1971, vol. 23, nº 4, p. 793, disponible à : https://www.persee.fr/doc/ridc_0035-3337_1971_num_23_4_16101.
Brandeis (L.) et Warren (S.), « The right to privacy », *Harvard Law Review* 1890, vol. 4, p. 193, disponible à : https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf.
Bredin (J.-D.), « Secret, transparence et démocratie », *Pouvoirs* 2001, nº 97, p. 5, disponible à : https://www.cairn.info/revue-pouvoirs-2001-2-page-5.htm.
Bretzner (J.-D.), « Ombres et lumières autour de la "qualité pour agir" dans l'action de groupe », *Gaz. Pal.* 2013, nº 136, p. 31.
Briat (M.) et **Pitrat** (C. M.), « Urgent, concepts à clarifier : protection de la vie privée et des données personnelles », *Droit de l'informatique et des télécoms* 1998, nº 3, p. 13.
Brisson (J.-F.), « Les pouvoirs de sanction des autorités de régulation et l'article 6 § 1 de la Convention européenne des droits de l'homme à propos d'une divergence entre le Conseil d'État et la Cour de cassation », *AJDA* 1999, p. 847.
Brownsword (R.), « Consent in data protection law : privacy, fair processing, and confidentiality », in *Reinventing Data Protection*, dir. **Gutwirth** (S.), **De Hert** (P.), **Nouwt** (S.), **Poullet** (Y.) et **Terwangne** (C. de), Springer, 2009, p. 157.
Brownsword (R.), « The cult of consent: fixation and fallacy », *Kings College Law Journal* 2004, vol. 15, nº 2, p. 223.
Bruguière (J.-M.), « "Droits patrimoniaux" de la personnalité. Plaidoyer en faveur de leur intégration dans une catégorie des droits de la notoriété », *RTD civ.* 2016, p. 1.
Bruguière (J.-M.), « Dans la famille des droits de la personnalité, je voudrais », *D.* 2011, p. 28.
Bruguière (J.-M.), « Le "droit à" l'oubli numérique, un droit à oublier », *D.* 2014, p. 299.
Brun (P.), « De la relativité des outils d'évaluation », *Gaz. Pal.* 2012, nº 315, p. 31.
Brunet (E.), « Les mécanismes de coopération des autorités de contrôle au sein de l'Union européenne et le Comité européen de la protection des données », *Revue de Droit International d'Assas* 2019, nº 2, p. 117, disponible à : https://www.u-paris2.fr/sites/default/files/document/cv_publications/rdia_ndeg2_2019.pdf.
Brunet (E.), « Règlement général sur la protection des données à caractère personnel – Genèse de la réforme et présentation globale », *Dalloz IP/IT* 2016, p. 567.
Brunet (F.), « Le champ d'application de la Charte de l'environnement », *AJDA* 2016, p. 1327.
Buat-Ménard (E.), « Open data des décisions de justice rendues en matière familiale », *AJ Fam.* 2019, p. 330.
Bygrave (L.) et **Wiese Schartum** (D.), « Consent, proportionnality and collective power », in *Reinventing Data Protection*, dir. **Gutwirth** (S.), **De Hert** (P.), **Nouwt** (S.), **Poullet** (Y.) et **Terwangne** (C. de), Springer, 2009, p. 157.
Campagne (N.), « La protection "informatique et libertés" des données des personnes morales en Europe », *RLDI* 2014, nº 104, p. 62.
Capurro (R.), « Past, present, and future of the concept of information », *Triple C* 2009, vol. 7, p. 125, disponible à : https://www.triple-c.at/index.php/tripleC/article/view/113.
Carbonnier (J.) obs. ss Cass. civ. 1re, 19 juill. 1960, *RTD civ.* 1961, p. 333.
Carbonnier (J.), « Effectivité et ineffectivité de la règle de droit », *L'année sociologique* 1957-1958, vol. 9, p. 3.
Carbonnier (J.), « En l'année 1817 », *Mélanges P. Raynaud*, Dalloz, 1985, p. 81.
Carbonnier (J.), note ss. Cass. civ. 1re, 19 juill. 1960, *RTD civ.* 1961 p. 333.
Caron (C.), « L'adage "les idées sont de libre parcours" utilisé pour sanctionner le plaideur paresseux », *CCE* 2013, nº 4, comm. 40.
Caron (C.), « Les morts n'ont pas de vie privée », *D.* 2000, p. 266.
Caron (C.), « Qualification de l'adresse "IP" : état des lieux jurisprudentiel », *CCE* 2007, nº 12, com. 144.
Caron (C.), « Validité des constats effectués par des agents assermentés », *CCE* 2009, nº 4, comm. 31.
Carre (S.), « Libre circulation des données, propriété et droit à l'information : à propos du règlement (UE) 2018/1807 du 14 novembre 2018 », *Dalloz IP/IT* 2020, p. 228.

Carrera Mariscal (A.), « Le CIL : modèle type du futur délégué à la protection des données ? », *Dalloz IP/IT* 2018, p. 233.
Cassuto (T.), « Usurpation d'identité numérique », *AJ pénal* 2010, p. 220.
Castets-Renard (C.), « Brève analyse du règlement général relatif à la protection des données personnelles », *Dalloz IP/IT* 2016, p. 331
Castets-Renard (C.), « Comment construire une intelligence artificielle responsable et inclusive ? », *D.* 2020, p. 225.
Castets-Renard (C.), « Invalidation du *Safe Harbor* par la CJUE : tempête sur la protection des données personnelles aux États-Unis », *D.* 2016, p. 88.
Castets-Renard (C.), « Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé : big data et open data », *RLDI* 2014, nº 108, p. 38.
Castets-Renard (C.), « Quels liens établir entre les USA et l'UE en matière de vie privée et protection des données personnelles ? », *Dalloz IP/IT* 2016, p. 115.
Catala (P.), « Ébauche d'une théorie juridique de l'information », *D.* 1984, p. 97.
Catala (P.), « La "propriété" de l'information », in *Mélanges P. Raynaud*, Dalloz, 1985, p. 97.
Catala (P.), « La transformation du patrimoine dans le droit civil moderne », *RTD civ.* 1966, p. 185.
Cate (F.), « The changing face of privacy protection in the European union and the United States », *Indiana Law Review* 1999, vol. 33, p. 173, disponible à : https://ssrn.com/abstract=933090.
Chacornac (J.), « L'articulation des répressions. Comment résoudre le problème de *non bis in idem* ? », *RSC* 2019, p. 333.
Champeil-Desplats (V.), « Effectivité et droits de l'homme : l'approche théorique », in *À la recherche de l'effectivité des droits de l'homme*, dir. Champeil-Desplats (V.) et Lochak (D.), Presses Universitaires de Paris Ouest, 2008, p. 11, disponible à : https://books.openedition.org/pupo/1152.
Charpenet (J.) et **Lequesne Roth** (C.), « Discrimination et biais genrés. Les lacunes juridiques de l'audit algorithmique », *D.* 2019, p. 1852.
Charrier (B.), « Le consentement exprimé par les mineurs en ligne », *Dalloz IP/IT* 2018, p. 333.
Charrière-Bournazel (C.), « L'oubli, l'histoire et le droit », colloque *Parole, tradition, transmission* de l'association AMA, Casablanca, 24 sept. 2005, disponible à : http://www.charriere-bournazel.com/loubli-lhistoire-et-le-droit/.
Chemillier-Gendreau (M.), « À propos de l'effectivité en droit international », *Revue belge de droit international* 1975, vol. 11, p. 38, disponible à : http://rbdi.bruylant.be/public/modele/rbdi/content/files/RBDI 1975/RBDI 1975-1/Etudes/RBDI 1975.1 - pp. 38 %C3%A0 46 - Monique Chemillier-Gendreau.pdf.
Chénédé (F.), « Responsabilité contractuelle et responsabilité extracontractuelle : une *summa divisio* ? », in *Vers une réforme de la responsabilité civile française*, dir. Mallet-Bricourt (B.), Dalloz, 2018, p. 31.
Chevallier-Govers (C.), « Le droit à la protection des données à caractère personnel : un droit fondamental du XXIe siècle ? » in *Enjeux et perspectives des droits de l'homme. L'Odyssée des droits de l'homme,* t. 3, dir. Ferrand (J.) et Petit (H.), L'Harmattan, 2003, p. 79.
Citron (D.), « Sexual privacy », *The Yale Law Journal* 2019, vol. 128, p. 1874, disponible à : https://digitalcommons.law.yale.edu/ylj/vol128/iss7/2/.
Citron (D.), « The privacy policymaking of State Attorneys General », *Notre Dame Law Review* 2017, vol. 92, p. 747, disponible à : https://scholarship.law.nd.edu/ndlr/vol92/iss2/5/.
Clément-Fontaine (M.), « L'union du droit à la protection des données à caractère personnel et du droit à la vie privée », *Légicom* 2017, nº 59, p. 61.
Clément-Fontaine (M.), « La convergence du droit de la propriété littéraire et artistique et du droit "droit des données" : une fatalité ? », in *Mélanges M. Vivant*, 2020, Dalloz, p. 97.
Cluzel-Métayer (L.) et **Debaets** (E.), « Le droit de la protection des données personnelles : la loi du 20 juin 2018 », *RFDA* 2018, p. 1101.
Cluzel-Métayer (L.), « Les limites de l'open data », *AJDA* 2016, p. 102.

Coeuret (A.), « Loi nº 91-491 du 15 mai 1991 modifiant le code de l'organisation judiciaire et instituant la saisine pour avis de la Cour de cassation », *RTD civ.* 1991, p. 615.
Cohen (D.), « Le juge européen et les données personnelles », in *Mélanges R. Badinter*, Dalloz, 2016, p. 249.
Cohen (D.), « Le juge, gardien des libertés ? », *Pouvoirs* 2009, nº 130, p. 113.
Cohen (J.), « What privacy is for », *Harvard Law Review* 2013, vol. 126, p. 1904, disponible à : https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_cohen.pdf.
Cohendet (M.-A.), « Légitimité, effectivité et validité », in *Mélanges P. Avril,* Paris, Montchrestien, 2001, p. 201.
Connallon (R.), « An integrative alternative for America's privacy torts », *Golden Gate University Law Review* 2007, vol. 38, p. 71, disponible à : https://digitalcommons.law.ggu.edu/ggulrev/vol38/iss1/3/.
Conte (P.), « "Effectivité", "inefficacité", "sous-effectivité", "surefficacité"… : variations pour droit pénal », in *Mélanges P. Catala,* Litec, 2001, p. 125.
Cope Huie (M.), **Laribee** (S.) et **Hogan** (S.), « The right to privacy in personal data : the EU prods the U.S. and controversy continues », *Tulsa Journal of Comparative and International Law* 2002, vol. 9, p. 391, disponible à : https://digitalcommons.law.utulsa.edu/tjcil/vol9/iss2/2.
Costaz (C.), « Le droit à l'oubli », *Gaz. Pal.* 1995, nº 207, p. 2.
Cousin (A.), « Réparer le préjudice causé par la violation du RGPD », *Dalloz IP/IT* 2019, p. 553.
Cousin (C.), « Le débat sur le référentiel indicatif de l'indemnisation du préjudice corporel des cours d'appel à l'heure des bases de données », *JCP G* 2017, nº 17, p. 483, disponible à : https://halshs.archives-ouvertes.fr/halshs-01513045/.
Croze (H.) ss Cass. crim., 29 avr. 1986, *JCP G* 1987, chron. 20788.
Cuzacq (N.), « Le mécanisme du *name and shame* ou la sanction médiatique comme mode de régulation des entreprises », *RTD com.* 2017, p. 473.
Cytermann (L.), « La loi Informatique et libertés est-elle dépassée ? », *RFDA* 2015, p. 99.
Dagot (M.), « Le nom des personnes morales », *JCP G* 1992, I, doctr. 3579.
Danis-Fatôme (A.), « Quelles actions judiciaires en cas de violation du RGPD ? », *CCE* 2018, nº 4, dossier 18.
Daoud (E.) et **Plénacoste** (F.), « Cybersécurité et objets connectés », *Dalloz IP/IT* 2016, p. 409.
Daragon (E.), « Étude sur le statut juridique de l'information », *D.* 1998, p. 63.
Debet (A.) et **Métallinos** (N.), « Mise en conformité RGPD / Analyse d'impact. La CNIL publie la liste des traitements pour lesquels une analyse d'impact relative à la protection des données (AIPD) est requise », *CCE* 2019, nº 1, comm. 4.
Debet (A.), « APB enfin remis en cause par la CNIL », *CCE* 2017, nº 12, comm. 101.
Debet (A.), « Autorités administratives indépendantes et personnalité morale », in *Travaux de l'Association Henri Capitant*, « La personnalité morale », t. 12, Journées nationales, Dalloz, 2010, p. 16.
Debet (A.), « Dans la famille Facebook, la CNIL s'intéresse désormais à WhatsApp », *CCE* mai 2018, nº 5, comm. 38.
Debet (A.), « La protection des données personnelles, point de vie du droit privé », *RDP* 2016, nº 1, p. 17.
Debet (A.), « Le consentement dans le RGPD : rôle et définition », *CCE* 2018, nº 4, dossier 9.
Debet (A.), « Les nouveaux instruments de conformité », *Dalloz IP/IT* 2016, p. 592.
Debet (A.), « Traitement de données aux fins de journalisme : état des lieux et perspectives », *Légipresse* 2020, hors-série nº 63, p. 51.
Debet (A.), « Un fichier non déclaré à la CNIL est une chose hors du commerce », *JCP G* 2013, nº 37, p. 930.
Debet (A.), « Une vidéo publiée sur YouTube est un traitement de données à des fins de journalisme », *CCE* 2019, nº 4, comm. 27.
Derieux (E.), « Vie privée et données personnelle – Droit à la protection et "droit à l'oubli" face à la liberté d'expression », *Les Nouveaux Cahiers du Conseil constitutionnel* 2015, nº 48,

p. 21, disponible à : https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/vie-privee-et-donnees-personnelles-droit-a-la-protection-et-droit-a-l-oubli-face-a-la-liberte-d.
Deroudille (A.) et **Fatah** (F.), « L'extraterritorialité du RGPD dans le contexte du "*Cloud Act*" », *RUE* 2019, p. 442
Deroulez (J.), « Les autorités de contrôles en droit des données personnelles », *CCE* 2018, nº 4, dossier 7.
Desgens-Pasanau (G.), « Contrôles et sanctions de la CNIL : quelles évolutions ? », *CCE* 2018, nº 4, dossier 17.
Desgorces (R.), « Les armes du juge judiciaire dans la protection des libertés fondamentales : le point de vue de la doctrine », in *Colloque La guerre des juges aura-t-elle lieu ? Analyse comparée des offices du juge administratif et du juge judiciaire dans la protection des libertés fondamentales,* dir. **Éveillard** (G.), 2016, disponible à : https://www.revuegeneraledudroit.eu/wp-content/uploads/coll_rennes_RGD201602.pdf.
Despax (M.), « La vie extraprofessionnelle du salarié et son incidence sur le contrat de travail », *JCP G* 1963, I, chron. 1776.
Destreguil (M.), « Plaidoyer en faveur d'une approche propriétariste des données personnelles », *Revue juridique personnes et famille* 2019, nº 3, p. 5.
Dezeuze (E.) et **Méléard** (C.), « Enquêtes et poursuites en matière d'abus de marché », *Revue des Sociétés* 2020, p. 556.
Dhenne (M.), « La loi nº 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires », *D.* 2018, p. 1817.
Dom (J.-P.), « Matérialité et localisation de l'entreprise numérique », *Dalloz IP/IT* 2019, p. 661.
Douville (T.), « Invalidation du *Privacy Shield* et insuffisance des clauses-types : fin (temporaire ?) des transferts de données à caractère personnel vers les États-Unis », *AJ Contrat* 2020, p. 436.
Douville (T.), « L'erreur de graphie d'un nom conduit le Conseil d'État à intensifier son contrôle des décisions de la CNIL », *Dalloz IP/IT* 2019, p. 115.
Douville (T.), « La protection des données à caractère personnel des mineurs et des majeurs protégés », *RLDC* 2018, nº 162, p. 42.
Douville (T.), « Les variations du droit au déréférencement », *D.* 2020, p. 515.
Dreveau (C.), « Réflexions sur le préjudice collectif », *RTD civ.* 2011, p. 249.
Dreyer (E.), « La fonction des droits fondamentaux dans l'ordre juridique », *D.* 2006, p. 748.
Drummond (F.), « Le fabuleux destin de la règle *non bis in idem* », *Bulletin Joly Bourse* 2014, nº 12, p. 605.
Dugué (M.), « La définition de la faute civile », *RDC* 2019, nº 116, p. 175.
Dumont (B.), « La régulation à l'échelle communautaire, une analyse économique des instruments et institutions de la protection des données au sein de l'UE », *Réseaux* 2011, nº 3, vol. 167, p. 49, disponible à : https://www.cairn.info/revue-reseaux-2011-3-page-49.htm.
Dumoulin (L.), « Les droits de la personnalité des personnes morales », *Revue des sociétés* 2006, p. 1.
Dupont-Lassalle (J.), « Protection des données personnelles », *Europe* 2014, nº 10, comm. 368.
Dupré de Boulois (X.), « Regard extérieur sur une jurisprudence en procès », *JCP G* 2016, nº 18, doctr. 552.
Durry (G.), « Rapport de synthèse », in *Le préjudice : questions choisies. Responsabilité civile et assurances* 1998, nº 5, p. 32.
Dyens (S.), « L'accès aux documents de gestion des agents des collectivités territoriales : entre transparence et confidentialité », *AJCT* 2011, p. 387.
Edelman (B.), « De la propriété-personne à la valeur-désir », *D.* 2004, p. 155.
Edelman (B.), « Entre le corps – objet profane – et le cadavre – objet sacré », *D.* 2010, p. 2754.
Esmein (P.), « La commercialisation du dommage moral », *D.* 1954, chron. 113.
Eynard (J.), « Une application systématique du RGPD ? », *Juris tourisme* 2018, nº 207, p. 19.

Fabre-Magnan (M.), « Le domaine de l'autonomie personnelle. Indisponibilité du corps humain et justice sociale », *D.* 2008, p. 31.
Fabre-Magnan (M.), « Le dommage existentiel », *D.* 2010, p. 2376.
Fairclough (B.), « Privacy piracy : the shortcomings of the United States' data privacy regime and how to fix it », *Journal of Corporation Law* 2016, vol. 42, p. 461.
Fasquelle (D.), « L'existence des fautes lucratives », *LPA* 20 nov. 2002, nº 232, p. 27.
Fauvarque-Cosson (B.) et **Maxwell** (W.), « Protection des données personnelles », *D.* 2018, p. 1033.
Fauvet (J.), « La protection des données personnelles », *RID comp.* 1987, vol. 39, nº 3, p. 551, disponible à : https://www.persee.fr/doc/ridc_0035-3337_1987_num_39_3_2724.
Favreau (A.), « Mort numérique : précisions sur la nature et le régime du contrôle *post mortem* des données à caractère personnel collectées », *RLDI* 2016, nº 132, p. 36.
Favro (K.), « La démarche de *compliance* ou la mise en œuvre d'une approche inversée », *Légicom* 2017, nº 59, p. 21.
Fittie-Duval (A.), « La théorie des apparences, nouveau paradigme de l'action publique ? », *AJDA* 2018, p. 440.
Flament (L.), « Les constatations visuelles effectuées sur Internet, sans recourir à un traitement préalable de surveillance automatisée, ne constituent pas un traitement de données à caractère personnel », *Dr. pén.* 2009, nº 5, étude 10.
Forest (D.), « Les limites intrinsèques de la garantie "d'indépendance" des autorités de contrôles. Le cas de la CNIL », *Dalloz IP/IT* 2016, p. 344.
Forest (D.), « Propos intempestifs sur les recours juridictionnels concernant les données personnelles », *RLDI* 2020, nº 166, p. 38.
Forest (D.), « Trente ans et des poussières. Retour sur les premiers pas de la CNIL », *RLDI* janv. 2008, nº 34, p. 77.
Forest (D), « Google et le "droit à l'oubli numérique" : genèse et anatomie d'une chimère juridique », *RLDI* 2014, nº 106, p. 76.
Foret (O.), « Le droit à l'oubli des mineurs », *Dalloz IP/IT* 2018, p. 350.
Foussard (D.), « La Cour de cassation et l'unification du droit », in *Les cours judiciaires suprêmes dans le monde arabe*, colloque de Beyrouth, 13 et 14 mai 1999, Bruylant, 2001, p. 161, disponible à : https://biblioteca.cejamericas.org/bitstream/handle/2015/2369/Lacourdecassationfrancaiseetlunificationdudroit.pdf?sequence=1&isAllowed=y.
Fraifield (J.) et **Engel** (C.), « Privacy as a public good », *Duke Law Journal* 2015, vol. 65, p. 385, disponible à : https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=3824&context=dlj.
Francillon (J.), « Infractions relevant du droit de l'informatique. La loi Informatique, fichiers et libertés du 6 janvier 1978 à l'épreuve de la jurisprudence pénale », *RSC* 1996, p. 676.
Frayssinet (J.), « L'utilité et les fonctions d'une formulation d'objectifs : l'exemple de la loi du 6 janvier 1978 », *Revue de la recherche juridique* 1984, nº 4, p. 903.
Frayssinet (J.), « La Cour de cassation et la loi informatique, fichiers et libertés, ou comment amputer une loi tout en raffermissant son application », *JCP G* 1988, I, p. 3323.
Frayssinet (J.), « La protection des données personnelles est-elle assurée sur l'Internet ? », in *Le droit international de l'Internet,* Bruylant, dir. G. Chatillon, 2003, p. 438.
Frayssinet (J.), « La régulation du respect de la loi Informatique, fichiers et libertés par le droit pénal : une épée de bois », *Légipresse* 2009, nº 42, p. 23, disponible à : https://www.cairn.info/revue-legicom-2009-1-page-23.htm.
Frayssinet (J.), « La traçabilité des personnes sur l'internet », *Dr et pat.* 2001, nº 93, p. 38.
Frayssinet (J.), « Le Conseil constitutionnel et la loi relative à l'informatique, aux fichiers et aux libertés (nº 92-316 DC, 20 janvier 1993) », *RFDC* 1993, nº 14, p. 398.
Fried (C.), « Privacy », *Yale Law Journal* 1968, vol. 77, p. 475, disponible à : https://digitalcommons.law.yale.edu/ylj/vol77/iss3/3/.

Frison-Roche (M.-A.), « Autorités administratives incomprises (AAI) », *JCP G* 2010, nº 48, p. 1166, disponible à : https://mafr.fr/IMG/pdf/63-_Autorites_Administratives_Incomprises_AAI_.pdf.
Frison-Roche (M.-A.), « Étude dressant un bilan des autorités administratives indépendantes », in **Gélard** (P.), « Rapport sur les autorités administratives indépendantes. Office parlementaire d'évaluation de la législation », Sénat, nº 404, 15 juin 2006, p. 75, disponible à : https://www.senat.fr/rap/r05-404-2/r05-404-21.pdf.
Frison-Roche (M.-A.), « L'efficacité des décisions en matière de concurrence : notions, critères, typologie », *LPA* 28 déc. 2000, nº 259, p. 4.
Frison-Roche (M.-A.), « Le droit de la *compliance* au-delà du droit de la régulation », *D.* 2018, p. 1561, disponible à : https://mafr.fr/media/assets/publications/frison-roche-m-a-le-droit-de-la-compliance-au-dela-du-droit-de-la-regulation-2018.pdf.
Frison-Roche (M.-A.), « Le pouvoir processuel des associations et la perspective de la *class action* », *LPA* 24 avr. 1996, nº 50, p. 28.
Frison-Roche (M.-A.), « Penser le monde à partir de la notion de "donnée" », in *Internet, espace d'interrégulation*, dir. **Frison-Roche** (M.-A.), Dalloz, 2016, p. 7, disponible à : https://mafr.fr/media/assets/publications/frison-roche-m-a-regulation-dun-monde-repense-comme-donnees-2016.0.pdf.
Frison-Roche (M.-A.), « Le droit de la *compliance* », *D.* 2016, p. 1871, disponible à : https://mafr.fr/media/assets/frison-roche-ma-le-droit-de-la-compliance-2016.pdf.
Frison-Roche (M.-A.), « Remarques sur la distinction de la volonté et du consentement en droit des contrats », *RTD civ.* 1995, p. 575, disponible à : https://mafrisonroche.phpnet.org/IMG/pdf/2-2.3_volont_consentement_1995.pdf.
G'sell (F.), « L'action des associations de consommateurs : à la recherche du groupe perdu », *Gaz. Pal.* 2014, nº 284, p. 15.
Gabrié (É.), « Les pouvoirs des autorités de protection des données », *Dalloz IP/IT* 2017, p. 268.
Gadbwa (T.), « Legislative update : Children's Online Privacy Protection Act of 1998 », *Children's Legal Rights Journal* 2016, vol. 36, p. 228, disponible à : https://lawecommons.luc.edu/clrj/vol36/iss3/7.
Galloux (J.-C.) et **Gaumont-Prat** (H.), « Droits et libertés corporels », *D.* 2010, p. 604.
Galloux (J.-C.), « Ébauche d'une définition juridique de l'information », *D.* 1994, p. 229.
Galloux (J.-C.), « L'adoption de la directive sur les secrets d'affaires », *RTD com.* 2017, p. 59.
Gassmann (H. P.), « Vers un cadre juridique international pour l'informatique et les autres techniques nouvelles de l'information », *Annuaire français de droit international* 1985, vol. 31, p. 747, disponible à : https://www.persee.fr/doc/afdi_0066-3085_1985_num_31_1_2685.
Gaudemet (M.) et **Perray** (R.), « "Scoring" et protection des données personnelles : un nouveau régime à l'efficacité incertaine », *LPA* 30 mai 2006, nº 107, p. 8.
Gaudemet (S.), « Nullité du contrat pour objet illicite. Un nouveau venu parmi les choses hors du commerce : le fichier non déclaré à la CNIL », *Revue juridique de l'économie publique* mars 2014, nº 717, comm. 12.
Gaullier (F.), « Le principe de finalité dans le RGPD : beaucoup d'ancien et un peu de nouveau », *CCE* 2018, nº 4, dossier 10.
Gauriau (B.) et **Teissier** (A.), « Données personnelles et économiques : l'interdiction de diffuser », *JCP S* 2020, nº 20-21, p. 2028.
Gautier (P.-Y.), « La preuve hors la loi ou comment, grâce aux nouvelles technologies, progresse la "vie privée" des salariés », *D.* 2001, p. 3148.
Gautier (P.-Y.), « Réseaux sociaux sur l'internet, données personnelles et droit des contrats », *D.* 2009, p. 616.
Gavalda (C.), « Le secret des affaires », in *Mélanges R. Savatier*, Dalloz, 1965, p. 291.
Gellert (R.), « Understanding the notion of risk in the general data protection regulation », *Computer Law & Security Review* 2018, vol. 34, nº 2, p. 279.
Gheorghe-Bădescu (I.), « Le droit à l'oubli numérique », *RUE* 2017, p. 153.
Glancy (D.), « The invention of the right to privacy », *Arizona Law Review* 1979, vol. 21, p. 1, disponible à : https://law.scu.edu/wp-content/uploads/Privacy.pdf.

Gleize (B.), « La personnalité numérique », in *Mélanges M. Vivant,* Dalloz, 2020, p. 189.
Godefroy (L.), « Le code algorithmique au service du droit », *D.* 2018, p. 734.
Godin (J.) et **Lemoalle** (E.), « Le rôle de *Data Protection Officer* à l'international, une étude comparative », *Dalloz IP/IT* 2018, p. 293.
Gola (R.), « Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », *Légicom* 2017, nº 59, p. 29.
Gout (O.), « L'émergence de nomenclatures relatives au dommage corporel », in *Le droit mis en barème ?,* dir. **Sayn** (I.), Dalloz, 2014, p. 227.
Gout (O.), « La nomenclature Dintilhac », *Gaz. Pal.* 2011, nº 358, p. 9.
Gratton (L.), « Le dommage déduit de la faute », *RTD civ.* 2013, p. 275.
Grégoire (S.), « Le statut de l'adresse IP : conséquences sur les mécanismes de constat, d'avertissement et de sanction du *peer to peer* envisagés par les accords de l'Élysée et le projet de loi "Création et Internet" », *Légicom* 2009, nº 43, p. 103.
Gridel (J.-P.), « Liberté de la presse et protection civile des droits modernes de la personnalité en droit positif français », *D.* 2005, p. 391.
Griguer (M.) et **Franco** (S.), « La CNIL durcit le ton en matière de sécurité. Étude comparative des sanctions prononcées à l'encontre des sociétés Uber et Bouygues Télécom », *Cahiers de droit de l'entreprise* 2019, nº 1, dossier 7.
Griguer (M.) et **Schwartz** (J.), « Privacy by design / Privacy by default. Une obligation de conformité et un avantage concurrentiel », *Cahiers de droit de l'entreprise* 2017, nº 3, p. 74.
Grzegorczyk (C.), « Le concept de bien juridique : l'impossible définition ? », in *Les biens et les choses, Archives de philosophie du droit* 1979, t. 24, Sirey, p. 258.
Guégan-Lécuyer (A.), « La qualité pour agir exclusivement réservée à certaines associations », *Gaz. Pal.* 2013, nº 136, p. 23.
Guerrier (C.), « Les aspects techniques de la régulation des données personnelles : la question du numéro IP », *Légicom* 2009, nº 42, p. 127.
Guinchard (S.), « Une *class action* à la française ? », *D.* 2005, p. 2180.
Gutwirth (S.) et **Gonzalez Fuster** (G.), « L'éternel retour de la propriété des données : de l'insistance d'un mot d'ordre », in *Liber amicorum Yves Poullet*. *Law, norms and freedoms in cyberspace*, dir. **Degrave** (E.), **Terwangne** (C. de), **Dusollier** (S.) et **Queck** (R.), Larcier, 2018, disponible à : https://works.bepress.com/serge_gutwirth/128/.
Haftel (B.), « Transferts transatlantiques de données personnelles : la Cour de justice invalide le *Safe Harbour* et consacre un principe de défiance mutuelle », *D.* 2016, p. 111.
Halpérin (J.-L.), « Diffamation, vie publique et vie privée en France de 1789 à 1944 », *Droit et cultures* 2013, vol. 63, p. 145, disponible à : https://journals.openedition.org/droitcultures/3073.
Halpérin (J.-L.), « L'essor de la "privacy" et l'usage des concepts juridiques », *Droit et Société* 2005, nº 61, p. 765, disponible à : https://www.cairn.info/article.php?ID_ARTICLE=DRS_061_0765.
Halpérin (J.-L.), « Protection de la vie privée et privacy : deux traditions juridiques différentes ? », *Les Nouveaux Cahiers du Conseil constitutionnel* 2015, nº 48, p. 59, disponible à : https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/protection-de-la-vie-privee-et-privacy-deux-traditions-juridiques-differentes.
Hauriou (M.), « De la personnalité comme élément de la réalité sociale », *Revue générale du droit* 1898, p. 20.
Hauser (J.), « L'indisponibilité relative des droits de la personnalité : conventions directes et indirectes sur le droit au respect de la vie privée et le droit au secret », *RTD civ.* 2000, p. 801.
Hauser (J.), « Les bornes de la personnalité juridique en droit civil », *Dr. Fam.* 2012, nº 9, dossier 4.
Hert (P. de) et **Gutwirth** (S.), « Data protection in the case law of Strasbourg and Luxembourg : constitutionalisation in action » in *Reinventing data protection ?,* dir. **Gutwirth** (S.), **Poullet** (Y.), **Hert** (P. de), **Terwangne** (C. de) et **Nouwt** (S.), Springer, 2009, p. 3.
Hetcher (S.), « The FTC as Internet privacy norm entrepreneur», *Vanderbilt Law Review* 2000, vol.53, p. 2041, disponible à : https://ssrn.com/abstract=253317.

Hilty (R.), « La privatisation de l'information par la propriété intellectuelle : problème et perspectives », *Revue internationale de droit économique* 2006, vol. 4, p. 353, disponible à : https://www.cairn.info/revue-internationale-de-droit-economique-2006-4-page-353.htm.
Hirsch (D.), « The law and policy of online privacy : regulation, self-regulation, or co-regulation ? », *Seattle University Law Review* 2011, vol. 34, p. 439, disponible à : https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=2003&context=sulr.
Hoang (C.), « In the middle : creating a middle road between U.S. and EU data protection policies », *National Administrative Law Judge Foundation* 2012, vol. 32, p. 810, disponible à : https://digitalcommons.pepperdine.edu/naalj/vol32/iss2/10.
Hostetler (D.) et **Okada** (S.), « Virtual solutions of the amended Children's Online Privacy Protection Act (COPPA) rule », *North Carolina Journal of Law & Technology Online* 2013, vol. 14, p. 167, disponible à : https://silo.tips/download/david-r-hostetler-seiko-f-okada.
Hu (R.), **Stalla-Bourdillon** (S.), **Yang** (M.), **Schiavo** (V.) et **Sassone** (V.), « Bridging policy, regulation and practice ? A techno-legal analysis of three types of data in the GDPR », in *Data protection and privacy. The age of intelligent machines*, dir. **Leenes** (R.), **Brakel** (R. van), **Gutwirth** (S.) et **De Hert** (P.), Bloomsbury Publishing, 2017, p. 126.
Huet (J.), « Des différentes sortes d'obligations et plus particulièrement de l'obligation de donner, la mal nommée, la mal aimée », *Mélanges J. Ghestin*, 2001, p. 425.
Huet-Weiller (D.), « La protection juridique de la voix humaine », *RTD civ.* 1982, p. 497.
Humbach (J.), « Privacy and the right to free expression », *First Amendment Law Review* 2012, vol. 11, p. 16, disponible à : https://ssrn.com/abstract=1996581.
Idoux (P.), « L'existence d'un contrôle juridictionnel restreint du refus d'enquêter opposé par la CNIL », *AJDA* 2012, p. 959.
Jack (A), « Les conventions relatives à la personne physique », *Revue critique de législation et de jurisprudence* 1933, p. 362, disponible à : https://gallica.bnf.fr/ark:/12148/bpt6k62550545/f367.image.r=Jack.
Jacob (P.), « La compétence des États à l'égard des données numériques : du nuage au brouillard… en attendant l'éclaircie ? », *Revue critique de droit international privé* 2019, p. 665.
Januel (P.), « L'affaire Benalla enflamme le Parlement », *Dalloz actualité* 20 juill. 2018, disponible à : https://www.dalloz-actualite.fr/flash/l-affaire-benalla-enflamme-parlement.
Jault-Seseke (F.) et **Zolynski** (C.), « Le Règlement 2016/679/UE relatif aux données personnelles. Aspects de droit international privé », *D.* 2016, p. 1874.
Jones (S.), « Reasonable expectations of privacy : searches, seizures, and the concept of Fourth amendment standing », *University of Memphis Law* Review 1997, vol. 27, p. 907.
Josserand (L.), « La personne humaine dans le commerce juridique », *D.* 1932, chron. 1.
Jourdain (P.), « Les droits de la personnalité à la recherche d'un modèle : la responsabilité civile », *Gaz. Pal.* 2007, nº 139, p. 52.
Jourdan-Marques (J.), « La publicité des décisions, une garantie émoussée ? », séminaire *L'avenir du procès civil* du Centre de recherche sur la Justice et le règlement des conflits de l'Université Paris II Panthéon Assas, *JCP G* 2019, supplément au nº 14, p. 62
Kalven (H.), « Privacy in tort law – were Warren and Brandeis wrong ? », *Law & Contemporary Problems* 1966, vol. 31, p. 326, disponible à : https://scholarship.law.duke.edu/lcp/vol31/iss2/7.
Kayser (P.) et **Frayssinet** (J.), « La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés », *RDP* 1979, p. 633.
Kayser (P.), « Aspects de la protection de la vie privée dans les sociétés industrielles », in *Mélanges G. Marty*, Université des sciences sociales de Toulouse, 1978, p. 725.
Kayser (P.), « Le secret de la vie privée et la jurisprudence civile », in *Mélanges R. Savatier*, Dalloz, 1965, p. 405.
Kayser (P.), « Les droits de la personnalité. Aspects théoriques et pratiques », *RTD civ.* 1971, p. 445.
Kerner (W), « A new (intellectual) property right for non-personal data ? An economic analysis », *Gewerblicher Rechtsschutz und Urheberrecht. Internationaler Teil* 2016, vol. 11,

p. 9, disponible à : https://www.uni-marburg.de/fb02/makro/forschung/magkspapers/paper_2016/37-2016_kerber.pdf.
Koops (B.-J.), « The trouble with European data protection law », *International Data Privacy Law* 2014, vol. 4, p. 250, disponible à : https://ssrn.com/abstract=2505692.
Koubi (G.), « Le fichier des "titres électroniques sécurisés" entériné », *JCP adm.* 2016, nº 47, p. 2300.
Labetoulle (D.), « Ni monstre, ni appendice : le "renvoi" de l'article 12 », *RFDA* 1988, p. 213.
Labrusse-Riou (C.) et **Bellivier** (F.), « Les droits de l'embryon et du fœtus en droit privé », *RID comp.* 2002, vol. 54, p. 579, disponible à : https://www.persee.fr/doc/ridc_0035-3337_2002_num_54_2_18757.
Labrusse-Riou (C.), « De quelques apports du droit des contrats au droit des personnes », in *Mélanges J. Ghestin*, LGDJ, 2001, p. 499.
Labrusse-Riou (C.), « L'anonymat du donneur : étude critique de droit positif français », in *Écrits de bioéthique,* dir. **Labrusse-Riou** (C.) et **Fabre-Magnan** (M.), Paris, PUF, 2007, p. 196.
Lambert-Garrel (L.) et **Vialla** (F.), « L'exception devient principe : à propos de la recherche sur l'embryon et les cellules souches embryonnaires. Proposition de loi adoptée le 16 juillet 2013 », *D.* 2013, p. 1842.
Lamberterie (I. de), « Informatique, libertés et opinions religieuses », *Archives des sciences sociales des religions* 1995, vol. 91, nº 1, p. 21, disponible à : https://www.persee.fr/doc/assr_0335-5985_1995_num_91_1_993.
Laneret (N.), « L'*accountability* et la protection effective des données personnelles dans un monde digital connecté », *RUE* 2020, p. 35.
Laneret (N.), **Knittel** (R.) et **Baudequin** (A.), « Protection des données personnelles : quand le droit de la concurrence s'en mêle », *Dalloz IP/IT* 2017, p. 619.
Lasserre Capdeville (J.), « La présence d'une adresse IP n'est pas une preuve suffisante en matière de virement », *Dalloz IP/IT* 2017, p. 661.
Laubadère (A. de), « Chronique générale de législation, Loi relative à l'informatique, aux fichiers et aux libertés », *AJDA* 1978, p. 146.
Laulom (S.), « L'indépendance affirmée de l'article 9 du code civil du droit commun de la responsabilité », *D.* 1997, p. 403.
Le Fur (L.), « Les caractère essentiels du droit en comparaison avec les autres règles de la vie sociale », *Archives de philosophie du droit et de sociologie juridique* 1935, p. 7, disponible à : https://gallica.bnf.fr/ark:/12148/bpt6k415557b/f5.item.
Le Tourneau (P.), « Des mérites et des vertus de la responsabilité civile », *Gaz. Pal.* 1985, II, p. 283.
Lebeau-Marianna (D.) et **Balducci** (A.), « UFC – Que Chosir contre Google + : la loi Informatique et libertés, un moyen supplémentaire de protection du consommateur ? », *Dalloz IP/IT* 2019, p. 258.
Leborgne (F.), « Le droit selon Henri Motulsky », *Revue juridique de l'Ouest* 2015, nº 2, p. 9.
Leclercq (P.), « Essai sur le statut juridique des informations », in *Les flux transfrontières de données : vers une économie informationnelle*, dir. **Madec** (A.), La Documentation française, 1982.
Lécuyer (H.), « Les autorités administratives indépendantes et le dualisme juridictionnel », *Revue de droit d'Assas* 2019, nº 18, p. 71, disponible à : https://www.u-paris2.fr/sites/default/files/document/brochures_plaquette/rda_18.pdf.
Leduc (F.), « Faut-il distinguer le dommage et le préjudice ? : point de vue privatiste », *Responsabilité civile et assurances* 2010, nº 3, dossier 3.
Lee (E.), « Recognizing rights in real time : the role of Google in the EU right to be forgotten », *University of California Davis Law Review* 2016, vol. 49, p. 1017, disponible à : https://lawreview.law.ucdavis.edu/issues/49/3/Articles/49-3_Lee.pdf.
Lenoir (N.), « Table-ronde », in *Colloque l'intérêt général, norme constitutionnelle ?,* dir. **Mathieu** (B.) et **Verpeaux** (M.), Dalloz, 2006, p. 82, disponible à : https://www.conseil-constitutionnel.fr/les-membres/l-interet-general-norme-constitutionnelle.

Lepage (A.), « L'article 226-2-1 du code pénal. Une nouvelle strate dans la protection pénale de la vie privée », *Dr. pén.* 2017, nº 1, étude 1.
Lepage (A.), « L'article 9 du code civil peut-il constituer durablement la "matrice" des droits de la personnalité ? », *Gaz. Pal.* 2007, nº 139, p. 43.
Lepage (A.), « Précisions sur les modes de réparation du préjudice en matière d'atteintes à la vie privée et à l'image », *D.* 2003, p. 1542.
Lepage (A.), « Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », *CCE* 2005, nº 2, étude 9.
Lepage (A.), « Vie privée. Condamnation du "coming out" forcé », *CCE* 2005, nº 3, comm. 48.
Lequette (S.), « La notion de contrat », *RTD civ.* 2018, p. 541.
Leroy (Y.), « La notion d'effectivité du droit », *Droit et société* 2011, nº 79, p. 715, disponible à : https://www.cairn.info/revue-droit-et-societe1-2011-3-page-715.htm.
Leroyer (A.-M.), « Embryon. Recherche. Cellules souches », *RTD civ.* 2013, p. 895.
Leroyer (A.-M.), « La notion d'état des personnes », in *Mélanges M. Gobert*, Economica, 2004, p. 247.
Lesaulnier (F.), « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz IP/IT* 2016, p. 573.
Lessi (J.), « La vie privée et les données personnelles dans l'espace numérique », *Revue Justice & Cassation* 2018, p. 65.
Lessig (L.), « Code is law. On liberty in cyberspace », *Harvard Magazine* janv. 2000, disponible à : « Code is law. On liberty in cyberspace ».
Letteron (R.), « Le droit à l'oubli », *Revue du droit public et de la science politique en France et à l'étranger* 1996, t. 112, p. 386.
Levinet (M.), « La notion d'autonomie personnelle dans la jurisprudence de la cour européenne des droits de l'homme », *Droits* 2009, nº 49, p. 3.
Lévy-Bruhl (H.), « La science du droit ou "juristique" », *Cahiers Internationaux de Sociologie* 1950, vol. 8, p. 123.
Lindon (R.), « La presse et la vie privée », *JCP G* 1965, I, doctr. 1887.
Lindsay (D.), « The relationship between general law protection of privacy and information privacy laws », in *Personal data & privacy protection*, dir. **Saad** (A.), LexisNexis, 2005, p. 29.
Link (R.), « Validity, Construction, and Application of Information Privacy Provisions of Gramm-Leach-Bliley Act », *American Law Reports* 2005, vol. 5, p. 497.
Listokin (S.), « Industry self-regulation of consumer data privacy and security », *The John Marshall Journal of Information Technology & Privacy Law* 2015, vol. 32, p. 15, disponible à : https://repository.jmls.edu/jitpl/vol32/iss1/2/.
Loiseau (G.), « Des droits humains pour personnes non humaines », *D.* 2011, p. 2558.
Loiseau (G.), « Droits de la personnalité. Janv. 2011 – déc. 2011 », *Légipresse* 2012, nº 290, p. 60.
Loiseau (G.), « La contractualisation des droits de la personnalité », *JCP G* 2012, nº 4, note 71.
Loiseau (G.), « La crise existentielle du droit patrimonial à l'image », *D.* 2010, p. 450.
Loiseau (G.), « La valeur contractuelle des conditions générales d'utilisation des réseaux sociaux », *CCE* 2012, nº 7-8, comm. 78.
Loiseau (G.), « Le droit à l'image aux prises avec la force obligatoire des conventions », *Dr et pat.* 2004, nº 127, p. 96.
Loiseau (G.), « Le rôle de la volonté dans le régime de protection de la personne et de son corps », *McGill Law Journal* 1992, vol. 37, nº 4, p. 965, disponible à : https://lawjournal.mcgill.ca/wp-content/uploads/pdf/6070392-Loiseau.pdf.
Loiseau (G.), « Les droits patrimoniaux de la personnalité en droit français », *Revue de droit de McGill* 1997, vol. 42, p. 319, disponible à : https://www.canlii.org/t/2pkz.
Loiseau (G.), « *Mortuorum corpus* : une loi pour le respect », *D.* 2009, p. 236.
Loiseau (G.), « Typologie des choses hors du commerce », *RTD civ.* 2000, p. 47.
Longobardi (N.), « Les autorités administratives indépendantes, une première approche (1re partie) », *LPA* 6 oct. 1995, nº 120, p. 4.

Lyon-Caen (G.), obs. ss Trib. Seine, 4 oct. 1965, *JCP* 1966, II, p. 14482.
Mackaay (E.), « La propriété est-elle en voie d'extinction ? », in *Nouvelles technologies et propriété*, actes du colloque tenu à Montréal, 9 et 10 nov. 1989, **Mackaay** (E.) (dir.), Litec, 1991, p. 217.
Mackay (E.), « Les biens informationnels ou le droit de suite dans les idées », in *L'appropriation de l'information*, dir. **Chamoux** (J.-P.), Librairies Techniques, 1986, p. 45, disponible à : http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/1986_03_45-65_Mackaay.pdf.
MacKinnon (C.), « Privacy v. Equality : Beyond Roe v. Wade », in *Feminism Unmodified. Discourses on life and law*, dir. **MacKinnon** (C.), Harvard University Press, 1988, p. 93.
Mainguy (D.), « À propos d'un "principe" préexistant à une loi », *D.* 2015, p. 246.
Mainguy (D.), « Introduction en droit français des *class actions* », *LPA* 22 déc. 2005, n° 254, p. 6.
Maisl (H.) et **Wiener** (C.), note ss CE Sec., 19 mai 1983, *D.* 1983, p. 546.
Maisl (H.), « La maîtrise d'une interdépendance. Commentaire de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés », *JCP G* 1978, I, p. 2891.
Malaurie (P.), « Les droits de la personnalité en 2003 », in *Mélanges A. Decocq,* Litec, 2004, p. 469.
Malaurie-Vignal (M.), « Réflexions sur la protection du patrimoine informationnel de l'entreprise contre le piratage économique », *D.* 2012, p. 1415.
Mallet-Poujol (N.), « Appropriation de l'information : l'éternelle chimère », *D.* 1997, p. 330, disponible à : http://www.jus.unitn.it/users/pascuzzi/privcomp00-01/topics/8/appr.htm.
Mallet-Poujol (N.), « Protection des données personnelles et droit à l'information », *Légicom* 2017, n° 59, p. 49.
Mantovani (M.), « Le RGPD en tant qu'espace juridique multi-échelle : quelles implications pour le droit international privé ? », *Revue de Droit International d'Assas* 2019, n° 2, p. 63, disponible à : http://communication.u-paris2.fr/medias/RDIA_n2_2019-2020.pdf.
Marais (A.), « Le droit à l'oubli numérique », in *La communication numérique, un droit, des droits*, dir. **Teyssié** (B.), Éd. Panthéon-Assas, 2012.
Marignol (L.), « Principe de responsabilité et action en responsabilité dans le Règlement général sur la protection des données (I) », *RLDI* 2020, n° 166, p. 44.
Marignol (L.), « Principe de responsabilité et action en responsabilité dans le Règlement général sur la protection des données (II) », *RLDI* 2020, n° 167, p. 54.
Marino (L.), « Comment mettre en œuvre le "droit à l'oubli" numérique ? », *D.* 2014, p. 1680.
Marino (L.), « Les nouveaux territoires des droits de la personnalité », *Gaz. Pal.* 2007, n° 139, p. 22.
Marino (L.), « Notre vie privée : des little data aux big data », colloque *Le secret à l'ère de la transparence* organisé par La Semaine Juridique, *JCP G* 2012, supplément au n° 47, p. 14, disponible à : https://drive.google.com/file/d/0B6ZbjsKP-QDTaXliSk9LeG4yMEE/edit.
Markale (J.), « Le nom, la parole et la magie », in *Corps Écrit* 1983, n° 8, p. 38.
Martial-Braz (N.) et **Rochfeld** (J.), « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte II : le droit à l'oubli numérique, l'éléphant et la vie privée », *D.* 2014, p. 1481.
Martial-Braz (N.), « Inconstitutionnalité du droit de communication des données de connexion reconnu à l'AMF », *Revue des Sociétés* 2017, p. 582.
Martial-Braz (N.), « L'abus de textes peut-il nuire à l'efficacité du droit ? La théorie du mille-feuille législatif à l'épreuve de la protection des données à caractère personnel », *Dalloz IP/IT* 2018, p. 459.
Martial-Braz (N.), « L'ambivalence du silence en droit des contrats », in *Le silence saisi par le droit privé,* dir. **Martial-Braz** (N.) et **Terryn** (F.), IRJS, 2014, p. 9.
Martial-Braz (N.), « L'extraterritorialité des décisions des autorités de régulation nationales : gage d'efficacité de la protection des données personnelles », *RUE* 2016, p. 288.
Martial-Braz (N.), « La transdisciplinarité du droit du numérique », in *Mélanges M. Vivant*, 2020, Dalloz, p. 849.

Martial-Braz (N.), « Le droit au déréférencement : vraie reconnaissance et faux-semblants ! », *Dalloz IP/IT* 2019, p. 631.
Martial-Braz (N.), « Le profilage. Fiche pratique », *CCE* 2018, nº 4, comm. 15.
Martial-Braz (N.), « Le renforcement des droits de la personne concernée », *Dalloz IP/IT* 2017, p. 253.
Martial-Braz (N.), « Les nouveaux droits des individus consacrés par la loi pour une République numérique. Quelle articulation avec le Règlement européen ? », *Dalloz IP/IT* 2016, p. 525.
Martial-Braz (N.), **Rochfeld** (J.) et **Gattone** (E.), « Quel avenir pour la protection des données à caractère personnel en Europe ? Les enjeux de l'élaboration chaotique du règlement 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 », *D.* 2013, p. 2788.
Martin (L.), « Le secret de la vie privée », *RTD Civ.* 1959, p. 225.
Martin-Laprade (B.), « Le filtrage des pourvois et les "avis" contentieux », *AJDA* 1988, p. 85.
Massot (J.), « La répartition entre les deux ordres », *RFDA* 2010, p. 907.
Matecki (L.), « Update : COPPA is ineffective legislation ! Next steps for protecting youth privacy rights in the social networking era », *Northwestern Journal of Law & Social Policy* 2010, vol. 5, p. 369, disponible à : https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1058&context=njlsp.
Mathey (N.), « L'uberisation et le droit des contrats : l'immixtion des plateformes dans la relation contractuelle », colloque *Le droit civil à l'ère du numérique* du Master 2 Droit privé général et du laboratoire de droit civil de l'Université Paris II Panthéon Assas, Paris, 21 avr. 2017, LexisNexis, p. 9, disponible à : https://web.lexisnexis.fr/fb/droit_civil_a_l_ere_numerique_112017/index.html#9.
Mathey (N.), « Les droits et libertés fondamentaux des personnes morales de droit privé », *RTD civ.* 2008, p. 205.
Mattatia (F.) et **Yaïche** (M.), « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? », *RLDI* 2015, nº 115, p. 63.
Mattatia (F.) et **Yaïche** (M.), « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? », *RLDI* 2015, nº 116, p. 41.
Mattatia (F.), « Données personnelles : la CJUE invalide le Privacy Shield », *JCP A* 2020, nº 36, act. 491.
Mattatia (F.), « L'adresse IP est-elle une donnée à caractère personnel ? », *Gaz. Pal.* 2008, nº 15, p. 9.
Maxwell (W.) et **Taïeb** (S.), « L'*accountability,* symbole d'une influence américaine sur le règlement européen des données personnelles ? », *Dalloz IP/IT* 2016, p. 123.
Maxwell (W.) et **Zolynski** (C.), « Protection des données personnelles », *D.* 2020, p. 1262.
Mazeaud (D.), « Vie privée des personnes publiques : toujours moins ? », *RTD civ.* 2018, p. 362.
Mazeaud (V.), « La constitutionnalisation du droit au respect de la vie privée », *Les Nouveaux Cahiers du Conseil constitutionnel* 2015, nº 48, p. 7, disponible à : https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/la-constitutionnalisation-du-droit-au-respect-de-la-vie-privee.
Mâzouz (A.), « Être ou ne plus être, les volontés à l'origine de la mort numérique », in *Droit et réseaux sociaux*, dir. **Ndior** (V.), Lextenso, 2015, p. 186.
Méadel (J.), « Faut-il introduire la faute lucrative en droit français ? », *LPA* 17 avr. 2007, nº 77, p. 6.
Métallinos (N.), « Anonymisation et pseudonymisation. Le Conseil d'État enterre l'analyse des flux piétons *via* WIFI », *CCE* 2017, nº 4, comm. 37.
Métallinos (N.), « Introduction d'une action de groupe en matière de violation de la loi Informatique et libertés », *CCE* 2016, nº 11, comm. 95.
Métallinos (N.), « La CJUE écarte l'approche téléologique de la notion de donnée à caractère personnel », *CCE* 2018, nº 3, comm. 23.

Métallinos (N.), « Les apports du règlement général relatif à la protection des données personnelles sur les conditions de licéité des traitements », *Dalloz IP/IT* 2016, p. 588.
Métallinos (N.), « Les leçons à tirer de la sanction de Google par la CNIL (1re partie : pas de « guichet unique » pour Google !) », *CCE* 2019, nº 5, comm. 35.
Métallinos (N.), « Maîtriser le risque Informatique et Libertés. La mise en place du correspondant à la protection des données personnelles », *Droit social* 2006, p. 378.
Métallinos (N.), « Tolérance zéro de la CNIL en cas de manquement élémentaire à la sécurité », *CCE* 2019, nº 9, comm. 56.
Meuris (F.), « Données publiques – "donnée" ouvre-toi ! », *CCE* 2014, nº 2, alerte 10.
Michel (A.), « Le traçage comportemental des internautes sur les réseaux sociaux : l'affaire des "cookies Facebook", véritable saga judiciaire ? », *Revue du droit des technologies de l'information* 2019, nº 74, p. 72, disponible à : http://www.crid.be/pdf/public/8524.pdf.
Molfessis (N.), « La réparation du préjudice extrapatrimonial », in *Les limites de la réparation du préjudice*, dir. **Ewald** (F.) *et al.*, Dalloz, 2009, p. 395.
Mongoin (D.), « Rapport introductif », in *La loyauté en droit public,* dir. **Hourson** (S.) et **Ferrari** (S.), Institut universitaire Varenne, 2018, p. 21.
Montecler (M.-C. de), « Le Conseil d'État donne une leçon d'Informatique et libertés à l'Éducation nationale », *AJDA* 2010, p. 1454.
Monteil (M.), « L'usurpation d'identité à l'épreuve du numérique », *D.* 2020, p. 101.
Montfort (P.), « Action de groupe à la française : garantir l'accès au juge », *Gaz. Pal.* 2013, nº 136, p. 27.
Mornet (B.), « Pour un référentiel national d'indemnisation du dommage corporel », *Gaz. Pal.* 2010, nº 153, p. 8.
Moron-Puech (B.), « De quelques faiblesses de la définition traditionnelle du contrat », *Droits* 2017, p. 115.
Morre (B.), « Contrat et religion. À la volonté de Dieu ou des contractants ? Commentaire sur l'affaire *Marcovitz* c. *Bruker* », *Revue juridique Thémis* 2009, vol. 43, p. 219, disponible à : https://ssl.editionsthemis.com/uploaded/revue/article/rjtvol43num1/moore.pdf.
Moshel (R.), « … and then there was one : the outlook for a self-regulatory United States amidst a global trend toward comprehensive data protection », *Texas Tech Law Review* 2005, vol. 37, p. 357.
Mouron (P.), « La protection des données personnelles dans l'environnement urbain. De la mesure d'audience publicitaire aux villes intelligentes », *RLDI* 2017, nº 139, p. 54.
Mouron (P.), « Pour ou contre la patrimonialité des données personnelles », *La revue européenne des médias et du numérique* 2018, nº 46-47, disponible à : https://la-rem.eu/2018/09/pour-ou-contre-la-patrimonialite-des-donnees-personnelles/.
Mousseron (J.-M.), **Raynard** (J.) et **Revet** (T.), « De la propriété comme modèle », in *Mélanges A. Colomer*, Litec, 1993, p. 281.
Mousseron (J.-M.), « Valeurs, biens, droits », in *Mélanges A. Breton et F. Derrida*, Dalloz, 1991, p. 277.
Mutua (M.), « The ideology of human rights », *Virginia Journal of International Law* 1996, vol. 36, p. 589, disponible à : https://ssrn.com/abstract=1525598.
Muzny (P.), « À quand une véritable culture des droits de l'homme en France ? », *JCP G* 2011, nº 38, p. 981.
Naftalski (F.), « L'impact du nouveau règlement sur les stratégies de transferts internationaux de données personnelles », *Dalloz IP/IT* 2016, p. 340.
Neirinck (C.), « L'embryon humain : une catégorie juridique à dimension variable ? », *D.* 2003, p. 841.
Nerson (R.), « Jurisprudence française en matière de droit civil », », *RTD civ.* 1966, p. 65.
Nerson (R.), « Jurisprudence française en matière de droit civil », *RTD civ.* 1968, p. 533.
Nerson (R.), « La protection de la vie privée en droit positif français », *RID comp.* 1971, vol. 23, nº 4, p. 737, disponible à : https://www.persee.fr/doc/ridc_0035-3337_1971_num_23_4_16099.
Netter (E.), « L'extinction du contrat et le sort des données personnelles », *AJ Contrat* 2019, p. 416, disponible à : https://hal.archives-ouvertes.fr/halshs-02450822.

Netter (E.), « La gestion par les responsables publics de leur réputation en ligne. Réflexions inquiètes sur les déséquilibres du droit au déréférencement », in colloque *La vie privée des responsables publics*, dir. **Sénac** (C.-E.), févr. 2019, Amiens, disponible à : https://hal.archives-ouvertes.fr/hal-02308919/document.
Netter (E.), « Sanction à 50 millions d'euros : au-delà de Google, la CNIL s'attaque aux politiques de confidentialité obscures et aux consentements creux », *Dalloz IP/IT* 2019, p. 165, disponible à : https://hal.archives-ouvertes.fr/hal-02314524.
Norodom (A.-T.), « Le standard européen de protection des données au regard du droit international », *Le règlement général sur la protection des données. Aspects institutionnels et matériels*, dir. **Brunessen** (B.) et **Bensamoun** (A.), Mare et Martin, 2020, p. 154.
Ochoa (N.), « La spécificité de la protection des données personnelles en matière fiscale. L'exemple de l'annulation probable du FATCA », *Gestion et Finances Publiques* 2016, n° 6, p. 75, disponible à : https://www.cairn.info/revue-gestion-et-finances-publiques-2017-6-page-75.htm.
Ochoa (N.), « Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition », *RFDA* 2015, p. 1157.
Ohm (P.), « Broken promises of privacy : responding to the surprising failure of anonymization », *UCLA Law Review* 2010, vol. 57, p. 1701, disponible à : https://ssrn.com/abstract=1450006.
Orif (V.), « L'élaboration dans la loi J21 d'un modèle général d'action de groupe : un essai à transformer », *Gaz. Pal.* 2017, n° 285, p. 80.
Pailler (L.), « L'applicabilité spatiale du Règlement général sur la protection des données (RGPD), commentaire de l'article 3 », *Journal du droit international* 2018, n° 3, doctr. 9.
Parker (R.), « A definition of privacy », *Rutgers Law Review* 1974, vol. 27, p. 275.
Passa (J.), « La propriété de l'information, un malentendu ? », *Dr. et Pat.* 2001, n° 91, p. 65.
Pastor (J.-M.), « La CNIL veut inscrire la protection des données dans la Constitution », *AJDA* 2008, p. 964.
Pellet (S.), « RGPD : l'effacement du consentement », *RGDA* 2019, n° 1, p. 6.
Pelletier (B.), « La protection de la vie privée au Canada », *Revue juridique Thémis* 2001, vol. 35, p. 485.
Pérès (C.), « Les données à caractère personnel et la mort. Observations relatives au projet de loi pour une République numérique », *D.* 2016, p. 90.
Peronne (G.) et **Daoud** (E.), « L'adresse IP est bien une donnée à caractère personnel », *Dalloz IP/IT* 2017, p. 120.
Péronne (G.) et **Daoud** (E.), « L'évolution du rôle du CIL à la lumière du nouveau règlement européen sur les données personnelles », *Dalloz IP/IT* 2016, p. 192.
Perray (R.) et **Salen** (P.), « La Cour de justice, les moteurs de recherche et le droit "à l'oubli numérique" : une fausse innovation, de vraies questions », *RLDI*, 2014, n° 109, p. 35.
Perray (R.) et **Uzan-Naulin** (J.), « Existe-t-il encore des données non personnelles ? », *Dalloz IP/IT* 2017, p. 286.
Perray (R.), « Le fichier TES : un réel danger ? », *D.* 2017, p. 56
Perray (R.), « Quelle stratégie pour les transferts de données personnelles hors de l'Union européenne à l'aune du RGPD », *CCE* 2018, n° 4, dossier 16.
Perreau (E.-H.), « Des droits de la personnalité », *RTD civ.* 1909, p. 501.
Perrin (J.-F.), « La notion d'"effectivité" en droit européen, international et comparé de la protection des données personnelles », in *Mélanges B. Dutoit,* Librairie Droz, 2002, p. 197.
Perthuis (C. de), « L'action collective à la française : étude de droit comparé entre le droit français et le droit américain », *LPA* 25 mars 2014, n° 60, p. 21.
Petit (F.), « Les droits de la personnalité confrontés au particularisme des personnes morales », *Dalloz Affaires* 1998, p. 826.
Peyrou (S.), « La protection des données à caractère personnel : un droit désormais constitutionnalisé et garanti par la CJUE », in *La protection des droits fondamentaux dans l'Union européenne*, dir. **Tinière** (R.) et **Vial** (C.), Bruylant, 2015, p. 213.
Pezard (A.), « Les limites à la protection – vers une nouvelle proportionnalité judiciaire », *Propriété Industrielle* 2018, n° 9, dossier 12.

Piccio (C.), « La réparation de l'atteinte aux droits de la personnalité », *Légipresse* 2010, nº 273, p. 74.
Piedelièvre (C.), « Barèmes médicaux-légaux et missions d'expertise : évolutions », *Gaz. Pal.* 2012, nº 315, p. 17.
Ponthoreau (M.-C.), « La protection des personnes contre les abus de l'informatique. À propos de la loi du 1er juillet 1994 relative au traitement des données nominatives ayant pour fin la recherche dans le domaine de la santé », *RFDA* 1996, p. 796.
Porchy-Simon (S.), « L'utilisation des barèmes en droit du dommage corporel », in *Le droit mis en barème ?,* dir. **Sayn** (I.), Dalloz, 2014, p. 201.
Post (R.), « Tensions entre "droit au débat public" et "droit au déréférencement". Regard d'outre-Atlantique », *RID comp.* 2017, nº 4, p. 821.
Poullet (Y.) et **Rouvroy** (A.), « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », in *État de droit et virtualité*, dir. **Benyekhlef** (K.) et **Trudel** (P.), Thémis, 2009, p. 157, disponible à : http://www.crid.be/pdf/public/6050.pdf.
Poullet (Y.), « La "propriété" des données. Balade au "pays des merveilles" à l'heure du *big data* », in *Mélanges M. Vivant*, 2020, Dalloz, p. 339.
Poullet (Y.), « Le fondement du droit à la protection des données nominatives : "propriété ou liberté" », *Nouvelles technologies et propriété*, actes du colloque tenu à Montréal, 9 et 10 nov. 1989, **Mackaay** (E.) (dir.), Litec, 1991, p. 175, disponible à : http://www.crid.be/pdf/public/6131.pdf.
Poullet (Y.), « Pour une troisième génération de règlementation de protection des données », in *Défis du droit à la protection de la vie privée*, dir. **Pérez Asinari** (M.) et **Palazzi** (P.), Bruylant, 2008.
Pousson-Petit (J.), « Le droit à l'anonymat », in *Mélanges L. Boyer*, PU Toulouse, 1996, p. 596.
Prévost (J.-B.), « Aspects philosophiques de la réparation intégrale », *Gaz. Pal.* 2010, nº 100, p. 7.
Prosser (W.), « Privacy », *California Law Review* 1960, vol. 48, p. 383, disponible à : https://lawcat.berkeley.edu/record/1109651.
Puillaude (S.), « La protection des données à caractère personnel : importation du modèle américain au sein de l'Union européenne », mémoire de Master 2 Paris II, 2016, disponible à : http://idc.u-paris2.fr/sites/default/files/memoires/memoire_sybille_pouillaude.pdf.
Purtova (N.), « The law of everyhting. Broad concept of personal data and future of EU data protection law », *Law, Innovation and Technology* 2018, nº 10, p. 1, disponible à : https://ssrn.com/abstract=3036355.
Quenaudon (R. de), « La cote mal taillée du salarié correspondant à la protection des données à caractère personnel », *Revue droit du travail* 2006, p. 32.
Rangeon (F.), « Réflexions sur l'effectivité du droit », in *Les usages sociaux du droit*, dir. **Lochak** (D.), Paris, PUF, 1989, p. 126, disponible à : https://www.u-picardie.fr/curapp-revues/root/23/rangeon.pdf.
Ravanas (J.), « Le plein exercice du droit au respect de la vie privée », *D.* 1998, p. 474.
Revet (T.), « La propriété de la personnalité », *Gaz. Pal.* 2007, nº 139, p. 49.
Revet (T.), « Le corps humain est-il une chose appropriée ? », *RTD civ.* 2017, p. 587.
Rias (N.), « Regard français », in *Quel avenir pour la responsabilité civile ?,* dir. **Lequette** (Y.) et **Molfessis** (N.), Dalloz, 2017, p. 63.
Ribes (D.), « Atteintes publiques et atteintes privées au droit au respect de la vie privée dans la jurisprudence du Conseil constitutionnel », *Les Nouveaux Cahiers du Conseil constitutionnel* 2015, nº 48, p. 35, disponible à : https://www.conseil-constitutionnel.fr/node/2329/pdf.
Richards (N.) et **Solove** (D.), « Prosser's privacy law : a mixed legacy », *California Law Review* 2010, vol. 98, p. 1887, disponible à : https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2104&context=faculty_publications.

Richards (N.), « Reconciling data privacy and the First amendment », *UCLA Law Review* 2005, vol. 52, p. 1149, disponible à : https://ssrn.com/abstract=598370.
Rigaux (F.), « L'élaboration d'un "right to privacy" par la jurisprudence américaine », *RID comp.* 1980, vol. 32, nº 4, p. 701, disponible à : https://www.persee.fr/doc/ridc_0035-3337_1980_num_32_4_3773.
Rigaux (F.), « Libre circulation des données et protection de la vie privée dans l'espace européen », in *La protection de la vie privée dans la société d'information*, t. 2, dir. **Tabatoni** (P.), Paris, PUF, 2002, p. 35, disponible à : https://academiesciencesmoralesetpolitiques.fr/wp-content/uploads/1999/01/tome-2.pdf.
Riklin (F.), « La protection des données personnelles : aspects de droit pénal. Situation actuelle en Suisse », *RID comp.* 1987, vol. 39, nº 3, p. 677, disponible à : https://www.persee.fr/doc/ridc_0035-3337_1987_num_39_3_2733.
Ripert (G.), « Le prix de la douleur », *D.* 1948, chron. 1.
Rivero (J.), « À propos de la loi Sécurité et liberté : filtrer le moustique et laisser passer le chameau. À propos de la décision du Conseil constitutionnel du 20 juin 1981 », *AJDA* 1981, p. 275.
Rivero (J.), « Sur l'effet dissuasif de la sanction juridique », in *Mélanges P. Raynaud*, Dalloz, 1985, p. 675.
Robinson (N.), **Graux** (H.), **Botterman** (M.) et **Valeri** (L.), « Review of the European data protection directive », *Rand Europe* 2009, p. 31, disponible à : https://www.rand.org/pubs/technical_reports/TR710.html.
Rocher (A.), « Les données personnelles des bénéficiaires effectifs de sociétés », *Revue des Sociétés* 2020, p. 139.
Rochfeld (J.), « Contre l'hypothèse de la qualification des données personnelles comme des biens », in *Les biens numériques,* dir. **Netter** (E.) et **Chaigneau** (A.), CEPRISCA, 2015, p. 221, disponible à : http://www.ceprisca.fr/wp-content/uploads/2016/03/2015-CEPRISCA-BIENS-NUMERIQUES.pdf.
Rochfeld (J.), « Du statut du droit contractuel "de protection de la partie faible" : les interférences du droit des contrats, du droit du marché et des droits de l'homme », in *Mélanges G. Viney*, LGDJ, 2008, p. 835.
Rochfeld (J.), « L'encadrement des décisions prises par algorithme », *Dalloz IP/IT* 2018, p. 474.
Rochfeld (J.), « La vie tracée ou le code civil doit-il protéger la présence numérique des personnes ? », in *Mélanges J. Hauser*, LexisNexis et Dalloz, 2012, p. 619.
Rochfeld (J.), « Le "contrat de fourniture de contenus numériques" : la reconnaissance de l'économie spécifique "contenus contre données" », *Dalloz IP/IT* 2017, p. 15.
Rochfeld (J.), « Une nouvelle source en droit des contrats : la loi Informatique et libertés », *RDC* 2014, nº 1, p. 119.
Roda (J.-C.), « Secret des affaires : et si l'on avait manqué l'essentiel ? », *D.* 2018, p. 1318.
Rodotà (S.), « Data protection as a fundamental right », in *Reinventing data protection ?,* dir. **Gutwirth** (S.), **Poullet** (Y.), **Hert** (P. de), **Terwangne** (C. de) et **Nouwt** (S.), Springer, 2009, p. 77.
Rogue (F.), « Capacité et consentement au traitement de données à caractère personnel et au contrat », *AJ Contrat* 2019, p. 370.
Rotenberg (M.), « Fair information Practices and the Architecture of Privacy (What Larry Doesn't Get) », *Stanford Technology Law Review* 2001, p. 1.
Roubier (P.), « Délimitation et intérêts pratiques de la catégorie des droits subjectifs », *Archives de philosophie du droit* 1964, t. 9, p. 83.
Rouhette (G.), « D'une faute, l'autre », *Droits* 1987, nº 5, p. 9.
Rousseau (D.), « Chronique de jurisprudence constitutionnel 1994-1995 », *Revue du droit public et de la science politique en France et à l'étranger* 1996, t. 112, p. 16.
Rouvroy (A.), « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data », in Conseil d'État, « Le numérique et les droits fondamentaux », *Rapport Public 2014*, La Documentation française, 2014, p. 416, disponible à : https://www.vie-publique.fr/sites/default/files/rapport/pdf/144000541.pdf.

Rouvroy (A.), « La robotisation de la vie ou la tentation de l'inséparation », in *L'intelligence artificielle et le droit*, dir. **Jacquemin** (H.) et **De Streel** (A.), Larcier, 2017, p. 34, disponible à : http://www.crid.be/pdf/public/8188.pdf.
Sacco (R.), « À la recherche de l'origine de l'obligation », *Archives de philosophie du droit* 2000, t. 44, p. 33, disponible à : http://www.philosophie-droit.asso.fr/APDpourweb/219.pdf.
Saint-Pau (J.-C.), « L'article 9 du Code civil : matrice des droits de la personnalité », *D.* 1999, p. 541.
Saint-Pau (J.-C.), « La distinction des droits de la personnalité et de l'action en responsabilité civile », in *Mélanges H. Groutel*, Litec, 2006, p. 405.
Sarda (F.), « Rapport français », in *Travaux de l'Association Henri Capitant*, « Les groupements », t. 45, Journées japonaises, Litec, 1994, p. 49.
Savatier (R.), « Vers de nouveaux aspects de la conception et de la classification juridique des biens corporels », *RTD civ.* 1958, p. 1.
Savatier (R.), obs. ss CA Paris, 23 mai 1924, *DP* 1925, p. 9.
Scaramozzino (E.), « *Open data* versus protection des données : les enjeux pour le tourisme des *smart cities* », *Juris tourisme* 2018, n° 207, p. 24.
Schwartz (P.) et **Peifer** (K.-N.), « Transatlantic data privacy », *Georgetown Law Journal* 2017, vol. 106, p. 115, disponible à : https://ssrn.com/abstract=3066971.
Schwartz (P.) et **Solove** (D.), « Reconciling personal information in the United States and European Union », *California Law Review* 2014, vol. 102, p. 877, disponible à : https://ssrn.com/abstract=2271442.
Schwartz (P.), « Privacy and democracy in cyberspace », *Vanderbilt Law Review* 1999, vol. 52, p. 1609, disponible à : https://ssrn.com/abstract=205875.
Schweiger (J.), « *Smart cities* et nouveaux enjeux de protection des données : comment tirer profit du nouveau règlement européen ? », *Dalloz IP/IT* 2017, p. 624.
Scottez (C.), « Le RGPD, un nouveau paradigme de la protection des données personnelles pour les professionnels et le régulateur », *Dalloz IP/IT* 2019, p. 229.
Sée (A.), « La régulation des algorithmes : un nouveau modèle de globalisation ? », *RFDA* 2019, p. 830.
Sénéchal (J.), « La fourniture de données personnelles par le client *via* Internet, un objet contractuel ? », *AJ Contrats d'affaires* 2015, p. 212.
Serafino (L.), « Arguing for protection of data stored in the cloud », *Pennyslvania Lawyer* 2013, vol. 35, p. 28.
Sériaux (A.), « La notion juridique de patrimoine », *RTD civ.* 1994, p. 801.
Serinet (A.), « L'instauration d'une répression des atteintes à l'intimité sexuelle par la loi pour une République numérique », *D.* 2016, p. 1711.
Seube (J.-B.), « La vente d'un fichier informatisé de clients non déclaré à la CNIL est annulée pour illicéité de son objet », *JCP E* juill. 2013, n° 29, p. 1422.
Sibony (A.-L.) et **Helleringer** (G.), « EU consumer protection and behavioural sciences : revolution or reform ? », in *Nudge and the law : a european perspective,* dir. **Alemanno** (A.) et **Sibony** (A.-L.), Hart Publishing, 2015, p. 209.
Simon (F.-L.) et **Bounedjoum** (A.), « RGPD : quelles règles en matière de responsabilité et quels impacts sur les contrats ? », *AJ Contrat* 2018, p. 172.
Solove (D.) et **Hartzog** (W.), « The FTC and the new common law of privacy », *Columbia Law Review* 2014, vol. 114, p. 583, disponible à : https://columbialawreview.org/content/the-ftc-and-the-new-common-law-of-privacy/.
Solove (D.), « Privacy self-management and the consent dilemma », *Harvard Law Review* 2013, vol. 126, p. 1880, disponible à : https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf.
Solove (D.), « The myth of the privacy paradox », *George Washington Law Review* 2021, vol. 89, disponible à : https://ssrn.com/abstract=3536265.
Spencer (S.), « Reasonable expectations and the erosion of privacy », *San Diego Law Review* 2002, vol. 39, p. 843, disponible à : https://ssrn.com/abstract=2015038.
Stalla-Bourdillon (S.) et **Knoight** (A.), « Anonymous data v. personal data. A false debate : an EU perspective on anonymization, pseudonymization and personal data », *Wisconsin*

International Law Journal 2017, vol. 34, p. 283, disponible à : https://repository.law.wisc.edu/s/uwlaw/media/77051.
Stoffel-Munck (P.), « Le préjudice moral des personnes morales », in *Mélanges P. le Tourneau*, 2008, p. 959.
Stoufflet (J.), « Le droit de la personne sur son image », *JCP* 1957, I, p. 1374.
Sudre (F.), « À propos du dynamisme interprétatif de la Cour européenne des droits de l'homme », *JCP G* 2001, nº 28, doctr. 335.
Sudre (F.), « Article II-67 », in *Traité établissant une Constitution pour l'Europe, commentaire article par article. Partie 2 : La Charte des droits fondamentaux*, t. 2, dir. **Burgorgue-Larsen** (L.), **Levade** (A.) et **Picod** (F.), Bruylant, 2005.
Sudre (F.), « La réécriture de la Convention par la Cour européenne des droits de l'homme », in *Mélanges J.-P. Costa*, Dalloz, 2011, p. 597.
Sudre (F.), « Le contrôle de proportionnalité de la Cour européenne des droits de l'homme. De quoi est-il question ? », *JCP G* 2017, nº 11, doctr. 289.
Swire (P.), « Financial privacy and the theory of high-tech government surveillance », *Washington University Law Quarterly* 1999, vol. 77, p. 461, disponible à : https://openscholarship.wustl.edu/law_lawreview/vol77/iss2/6.
Swire (P.), « The surprising virtues of the new financial privacy law », *Minnesota Law Review* 2002, vol. 86, p. 1263, disponible à : https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=3082&context=mlr.
Swire (P.), **Hemmings** (J.) et **Vergnolle** (S.), « A mutual legal assistance case study : the United States and France », *Wisconsin International Law Journal* 2017, vol. 42, p. 323, disponible à : https://ssrn.com/abstract=2921289.
Taillefait (A.), « La mobilité entre le secteur public et le secteur privé : évolution ou agitation ? », *AJDA* 2018, p. 559.
Tambou (O.), « L'émergence d'un modèle européen d'interrégulation en matière de protection des données personnelles », *Mélanges J. Monéger*, 2017, LexisNexis, p. 382, disponible à : https://hal.archives-ouvertes.fr/hal-01529151.
Tambou (O.), « Protection des données personnelles : les difficultés de la mise en œuvre du droit européen au déréférencement », *RTD eur.* 2016, p. 249, disponible à : https://hal.archives-ouvertes.fr/hal-01408535.
Teller (M.), « Les difficultés de l'identité numérique : quelle qualification juridique pour l'adresse IP ? », *D.* 2009, p. 1988.
Thérard-Jallu (C.), **Job** (K.-M.) et **Mintz** (S.), « Invalidation de l'accord *Safe Harbor* par la CJUE : portée, impacts et premiers éléments de solution », *Dalloz IP/IT* 2016, p. 26.
Torck (S.), « L'exécution et la contestation des opérations de paiement », *JCP E* 2010, nº 2, p. 1033.
Tracol (X.), « Le règlement et la directive relatifs à la protection des données à caractère personnel », *Europe* 2016, nº 10, étude 8.
Trudel (P.), « La protection de la vie privée dans les systèmes d'information relatifs à la santé. Ajuster les concepts aux réalités des réseaux », in *Les pratiques de recherche biomédicales visitées par la bioéthique*, dir. **Hervé** (C.), **Knoppers** (B.-M.) et **Molinari** (P.), Dalloz, 2003, p. 166.
Tunc (A.), « Responsabilité civile et dissuasion des comportements antisociaux », in *Mélanges M. Ancel*, t. 1, Pédone, 1975, p. 407.
Vadillo (F.), « Liberté individuelle vs liberté personnelle : l'article 66 de la Constitution dans la jurisprudence du Conseil constitutionnel ou la progressive reconnaissance d'un habeas corpus à la française », *LPA* 22 avr. 2015, nº 80, p. 4.
Vatier (B.), « Peut mieux faire ! », *Gaz. Pal.* 2013, nº 136, p. 53.
Vercken (G.), **Van Ossel** (G.) et **Serpagli** (C.), « Le "correspondant à la protection des données" : une création inachevée ? », *RLDI* 2005, nº 9, p. 58.
Verdier (H.) et **Vergnolle** (S.), « L'État et la politique d'ouverture en France », *AJDA* 2016, p. 92.
Vier (C.-L.), « La notion de conflit d'intérêts », *AJDA* 2012, p. 869.
Vignal (N.), « L'accès au dossier médical », *LPA* 19 juin 2002, nº 122, p. 19.

Viney (G.), « L'action d'intérêt collectif et le droit de l'environnement écologique et sa réparation. Rapport français », in *Les responsabilités environnementales dans l'espace européen,* dir. Dubuisson (B.) et Viney (G.), Bruylant, 2006, p. 223.
Vivant (M.) et **Lucas** (A.), « Droit de l'informatique (suite) », *JCP E*, 1990, p. 15761.
Vivant (M.), « À propos des "biens informationnels" », *JCP G* 1984, I, p. 3132.
Vivant (M.), « L'État de non-droit », *D.* 2019, p. 753.
Vivant (M.), « Le patronyme saisi par le patrimoine », in *Mélanges A. Colomer*, Litec, 1993, p. 517.
Von Jhering (R.), « De l'intérêt dans les contrats, et de la prétendue nécessité de la valeur patrimoniale des prestations obligatoires », dans *Œuvres choisies*, vol. II, Librairie A. Marescq, 1893, disponible à : https://archive.org/details/uvreschoisiestr00meulgoog/page/n160.
Wachter (S.), **Mittlestadt** (B.) et **Floridi** (L.), « Why a right to explanation of automated decision-making does not exist in the general data protection regulation », *International Data Privacy Law* 2017, vol. 7, p. 76, disponible à : https://doi.org/10.1093/idpl/ipx005.
Waquet (P.), « La vie personnelle du salarié », in *Mélanges J.-M. Verdier,* Dalloz, 2001, p. 513.
Watkins (J.), « No good deed goes unpunished : the duties held by malware researchers, penetration testers, and "white hat" hackers », *Minnesota Journal of Law, Science & Technology* 2018, vol. 19, p. 535, disponible à : https://scholarship.law.umn.edu/mjlst/vol19/iss2/7.
Wester-Ouisse (V.), « Le préjudice moral des personnes morales », *JCP G* 2003, nº 26, doctr. 145.
Whitman (J.), « The two western cultures of Privacy : dignity versus liberty », *The Yale Law Journal* 2004, vol. 113, p. 1151, disponible à : https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1647&context=fss_papers.
Wiederkehr (G.), « La légitimité de l'intérêt pour agir », in *Mélanges S. Guinchard*, 2010, Dalloz, p. 877.
Wienczyslaw (W.), « Le "droit à l'intimité" aux États-Unis », *RID comp.* 1965, vol. 17, nº 2, p. 365, disponible à : https://www.persee.fr/doc/ridc_0035-3337_1965_num_17_2_14193.
Wilkins (R.), « Defining the "reasonable expectation of privacy" : an emerging tripartite analysis », *Vanderbilt Law Review* 1987, vol. 40, p. 1077, disponible à : https://scholarship.law.vanderbilt.edu/vlr/vol40/iss5/2/.
Zarsky (T.), « Privacy and manipulation in the digital age », *Theoretical Inquiries in Law* 2019, vol. 20, p. 158, disponible à : https://ssrn.com/abstract=3321172.
Zenati (F.), « La saisine pour avis de la Cour de cassation », *D.* 1992, p. 247.
Zoller (É.), « Cour suprême des États-Unis : Session d'octobre 2017 », *RDP* 2018, nº 6, p. 1761.
Zoller (É.), « Transparence et démocratie : généalogie d'un succès », in *Transparence, démocratie et gouvernance citoyenne,* dir. **Guglielmi** (G.) et **Zoller** (É.), Éd Panthéon-Assas, 2014, p. 13.
Zolynski (C.), « La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne », *Dalloz IP/IT* 2020, p. 429.
Zolynski (C.), « Les nouveaux contours de l'action de groupe et de l'action collective au lendemain de la loi pour la protection des données : un *empowerment* renforcé », *Dalloz IP/IT* 2018, p. 470.
Zolynski (C.), « Protection des consommateurs – Contrats de fourniture de contenus et de services numériques. À propos de la directive 2019/770/UE – Aperçu rapide », *JCP G* 2019, nº 47, p. 1181.
Zolynski (C.), **Le Roy** (M.) et **Levin** (F.), « L'économie de l'attention saisie par le droit », *Dalloz IP/IT* 2019, p. 614.
Zorn (C.), « Le jeu de données composites : données personnelles et (en même temps) non personnelles ? », *Dalloz IP/IT* 2020, p. 420.

B. Extra-juridiques

Abowd (J.), « The U.S. census bureau adopts differential privacy », in *KDD' 18*, Londres, août 2018, disponible à : https://digitalcommons.ilr.cornell.edu/cgi/viewcontent.cgi?article=1050&context=ldi.
Adomavicius (G.), **Bockstedt** (J.), **Curley** (S.) et **Zhang** (J.) et Ransbotham (S.), « The hidden side effects of recommendation systems », *MIT Sloan Management Review* 2019, p. 19, disponible à : http://mobileservices.texterity.com/mitsmr/winter_2019/MobilePagedArticle.action?articleId=1449479&app=false#articleId1449479.
Adomavicius (G.), **Bockstedt** (J.), **Curley** (S.) et **Zhang** (J.), « Effects of online recommendations on consumers' willingness to pay », *Management Science* 2017, vol. 64, nº 11, disponible à : https://ssrn.com/abstract=2982194.
Amadieu (J.-B.), « Nos censures au miroir de l'Index librorum prohibitorum », *Raisons politiques* 2016, disponible à : https://www.cairn.info/revue-raisons-politiques-2016-3-page-67.htm.
Appourchaux (K.), « Neurosciences et techniques de redirection de l'attention : redéfinir le libre arbitre en termes d'apprentissage de la maîtrise de nos capacités attentionnelles », *Psychiatrie, Sciences humaines, Neurosciences* 2013, vol. 11, p. 43, disponible à : https://www.cairn.info/revue-psn-2013-4-page-43.htm.
Baldner (J.-M.), « Sur la naissance de l'individu », *Espace temps* 1988, vol. 37, p. 25, disponible à : https://www.persee.fr/doc/espat_0339-3267_1988_num_37_1_3400.
Balima (S. T.), « Une ou des "sociétés de l'information" ? », *Hermès La Revue* 2004, nº 40, p. 205, disponible à : https://www.cairn.info/revue-hermes-la-revue-2004-3-page-205.htm.
Beauvallet (G.), **Flichy** (P.) et **Ronai** (M.), « Incorporer la protection de la vie privée dans les systèmes d'information, une alternative à la régulation par la loi ou par le marché », *Terminal* 2003, nº 88, p. 89.
Bertram (T.) *et al.*, « The five years of the right to be forgotten », *CCS'* nov. 2019, Londres, disponible à : https://research.google/pubs/pub48483/.
Béru (L.), « Statistiques ethniques, débats sociétaux et études en communication. L'universalisme français à la lumière du différentialisme anglo-saxon », *Médiation & Information* 2008, nº 28, p. 53, disponible à : https://www.mei-info.com/wp-content/uploads/revue28/5MEI-28.pdf.
Bird (S.), **Segall** (I.) et **Lopatka** (M.), « Replication : why we still can't browse in peace. On the uniqueness and reidentifiability of Web browsing histories », *6th Symposium on Usable Privacy and Security* 2020, disponible à : https://www.usenix.org/system/files/soups2020-bird.pdf.
Bonawitz (K.), **Ivanov** (V.), **Kreuter** (B.), **Marcedone** (A.), **McMahan** (H. B.), **Patel** (S.), **Ramage** (D.), **Segal** (A.) et **Seth** (K.), « Privacy secure agregation for privacy-preserving machine learning », *CCS'* oct. 2017, Dallas, disponible à : https://eprint.iacr.org/2017/281.pdf.
Cardon (D.) et **Crépel** (M.), « Les algorithmes et la régulation des territoires », in *Gouverner la ville numérique*, dir. **Courmont** (A.) et **Le Galès** (P.), PUF, 2019, disponible à : https://laviedesidees.fr/Algorithmes-et-regulation-des-territoires.html.
Casilli (A.), « Contre l'hypothèse de la "fin de la vie privée". La négociation de la *privacy* dans les médias sociaux », *Revue française des sciences de l'information et de la communication* 2013, nº 3, disponible à : https://doi.org/10.4000/rfsic.630.
Chellappa (R.), **Sinha** (P.) et **Jonathon Philips** (P.), « Face recognition by computers and humans », *IEEE Computer Society* 2010, vol. 43, nº 2, p. 46, disponible à : http://pages.cs.wisc.edu/~dyer/cs534-fall11/papers/face-recog-2010.pdf.
Colangelo (G.) et **Maggiolino** (M.), « Data accumulation and the privacy – antitrust interface : insights from the Facebook case », *International Data Privacy Law* 2018, vol. 8, p. 224, disponible à : https://ssrn.com/abstract=3125490.
Courmont (A.), « Plateforme, *big data* et recomposition du gouvernement urbain : les effets de Waze sur les politiques de régulation du trafic », *Revue française de sociologie* 2018, vol. 59, p. 423.

Covington (P.), **Adams** (J.) et **Sargin** (E.), « Deep neural networks for YouTube recommandations », *RecSys* sept. 2016, disponible à : https://dl.acm.org/doi/10.1145/2959100.2959190.
Davidson (J.), **Liebald** (B.), **Liu** (J.), **Nandy** (P.) et **Van Vleet** (T.), « The YouTube video recommandation system », *RecSys* sept. 2010, disponible à : https://www.inf.unibz.it/~ricci/ISR/papers/p293-davidson.pdf.
Deffuant (G.), **Neau** (D.), **Amblard** (F.) et **Weisbuch** (G.), « Mixing Beliefs among Interacting Agents », *Advances in Complex Systems* 2000, vol. 3, nº 1, p. 87, disponible à : http://wwwlisc.clermont.cemagref.fr/imagesproject/finalreport/mixbel.pdf.
Deleuze (G.), « Post-scriptum sur les sociétés de contrôle », *Pourparlers* 1990, disponible à : https://infokiosques.net/IMG/pdf/Deleu.pdf.
Denis (V.), « Petite histoire des documents d'identité : la France des Lumières », *Documentaliste-Sciences de l'Information* 2010, vol. 47, p. 32, disponible à : https://www.cairn.info/revue-documentaliste-sciences-de-l-information-2010-1-page-32.htm#re6no6.
Delage (P.-J.), « Respect des morts, dignité des vivants », *D.* 2010, p. 2044.
Delisle (E.), « Le nouveau rôle de la CNIL », *Jurisport* 2019, nº 196, p. 32.
Delzangles (B.), « Effectivité, efficacité et efficience dans la jurisprudence de la Cour européenne des droits de l'homme », in *À la recherche de l'effectivité des droits de l'homme*, dir. **Champeil-Desplats** (V.) et **Lochak** (D.), Presses Universitaires de Paris Ouest, 2008, p. 41, disponible à : https://books.openedition.org/pupo/1158.
Delzangles (H.), « Un vent d'impartialité souffle encore sur le droit de la régulation », *AJDA* 2014, p. 1021.
Descartes (R.), « Meditationes de prima philosophia. Secudae Responsines », in *Œuvres*, vol. VII, dir. **Adam** (C.) et **Tannery** (P.), Vrin, 1996.
Dubey (G.), « Nouvelles techniques d'identification, nouveaux pouvoirs. Le cas de la biométrie », *Cahiers internationaux de sociologie* 2008, nº 125, p. 263, disponible à : https://www.cairn.info/revue-cahiers-internationaux-de-sociologie-2008-2-page-263.htm.
Dwork (C.), « Differential privacy », in *International Colloquium on Automata, Languages, and Programming*, Springer, 2006.
Engelsma (J.), **Arora** (S.), **Jain** (A.) et **Paulter** (N.), « Universal 3D wearable fingerprint targets : advancing fingerprint reader evaluations », *IEEE Transactions on Information Forensics and Security* 2018, vol. 13, nº 6, disponible à : http://biometrics.cse.msu.edu/Publications/Fingerprint/EngelsmaAroraJainPaulter_Universal3DWearableFingerprintTargetsAdvancingFingerprintReaderEvaludations_TIFS2018.pdf.
Filippi (P. de), « Gouvernance algorithmique : vie privée et autonomie individuelle à l'ère des *Big Data* », in *Open data & data protection : nouveaux défis pour la vie privée*, dir. **Bourcier** (D.) et **Filippi** (P. de), Mare & Martin, 2016, disponible à : https://hal.archives-ouvertes.fr/hal-01382010/document.
Genet (J.-P.), « La genèse de l'État moderne. Les enjeux d'un programme de recherche », *Actes de la Recherche en Sciences Sociales* 1997, p. 6.
Georges (F.), « Représentation de soi et identité numérique. Une approche sémiotique et quantitative de l'emprise culture du web 2.0 », *Réseaux* 2009, nº 154, p. 165, disponible à : https://www.cairn.info/revue-reseaux-2009-2-page-165.htm.
Gomez-Uribe (C.) et **Hunt** (N.), « The Netflix recommender system : algorithms, business value, and innovation », *ACM Transactions on Management Information Systems* 2015, vol. 6, nº 4, article 13, disponible à : https://dl.acm.org/doi/10.1145/2843948.
Granjon (F.) et **Denouël** (J.), « Exposition de soi et reconnaissance de singularités subjectives sur les sites de réseaux sociaux », *Sociologie* 2010, vol. 1, p. 25, disponible à : https://www.cairn.info/revue-sociologie-2010-1-page-25.htm.
Grimmelmann (J.), « The structure of search engine law », *Iowa Law Review* 2007, vol. 93, p. 1, disponible à : https://ssrn.com/abstract=979568.
Guichard (C.), « La signature dans le tableau aux XVII^e^ et XVIII^e^ siècles : identité, réputation et marché de l'art », *Sociétés et représentations* 2008, nº 25, p. 47, disponible à : https://www.cairn.info/journal-societes-et-representations-2008-1-page-47.htm.

Haim (M.), **Graefe** (A.) et **Brosius** (H.-B.), « Burst of the filter bubble ? Effects of personalization on the diversity of Google News », *Digital Journalism* 2016, vol. 6, nº 3, p. 330, disponible à : https://www.researchgate.net/publication/318256136_Burst_of_the_Filter_Bubble_Effects_of_personalization_on_the_diversity_of_Google_News.
Hanson (J) et **Kysar** (D.), « Taking behavioralism seriously : the problem of market manipulation », *New York University Law Review* 1999, vol. 74, p. 630, disponible à : https://www.nyulawreview.org/wp-content/uploads/2018/08/NYULawReview-74-3-Hanson-Kysar.pdf.
Héran (F.), « France/États-Unis : deux visions de la statistique des origines et des minorités ethniques », *Santé, Société et Solidarité* 2005, nº 1, p. 167, disponible à : https://www.persee.fr/doc/oss_1634-8176_2005_num_4_1_1038.
Hildebrand (C.) et **Schlager** (T.), « Focusing on others before you shop : exposure to Facebook promotes conventional product configurations », *Journal of the Academy of Marketing Science* 2019, vol. 47, p. 291.
Introna (L.) et **Nissenbaum** (H.), « Shaping the Web : why the politics of search engines matters », *The Information society* 2000, vol. 16, p. 1, disponible à : https://ssrn.com/abstract=222009.
Jeskanen-Sundström (H.), « ICT Statistics at the New Millennium. Developing Official Statistics. Measuring the Diffusion of ICT and its Impacts », *IAOS* 2001, Japon, disponible à : https://www.stat.go.jp/english/info/meetings/iaos/pdf/jeskanen.pdf.
Kelly (J.) et **François** (C.), « This is what filter bubbles actually look like. Maps of Twitter activity show how political polarization manifests only and why divides are so hard to bridge », *MIT Tech Review* 2018, vol. 121, disponible à : https://www.technologyreview.com/2018/08/22/140661/this-is-what-filter-bubbles-actually-look-like/.
Kramer (A.), **Guillory** (J.) et **Hancock** (J.), « Experimental evidence on massive-scale emotional contagion through social networks », *Proceedings of the National Academy of Sciences of the United States of America* 2014, vol. 111, p. 8788, disponible à : https://www.pnas.org/content/pnas/111/24/8788.full.pdf.
Le Crosnier (H.), « La documentarisation des humains », *Documentaliste-Sciences de l'Information* 2010, vol. 47, p. 34, disponible à : https://www.cairn.info/revue-documentaliste-sciences-de-l-information-2010-1-page-32.htm#re6no6.
Le Crosnier (H.), « Usage des traces par la publicité comportementale », in *Traces numériques. De la production à l'interprétation,* dir. **Galinon-Melenec** (B.) et **Zlitni** (S.), CNRS, 2013, p. 91, disponible à : https://books.openedition.org/editionscnrs/21741.
McDonald (A.) et **Faith Cranor** (L.), « The cost of reading privacy policies », *I/S: A Journal of Law and Policy for the Information Society* 2008-2009, vol. 4, p. 543, disponible à : https://hdl.handle.net/1811/72839.
Ménard (M.), « Autoroutes de l'information et société de l'information : pour un renversement de perspective », in *Les autoroutes de l'information : enjeux et défis,* dir. **Frémont** (J.) et **Ducasse** (J.-P.), Université de Montréal, 1996, p. 103.
Merzeau (L.), « De la surveillance à la veille », in dossier « Internet et la société de contrôle : le piège ? », dir. **Damien** (R.) et **Mathias** (P.), *Cités* 2009, nº 39, p. 67, disponible à : https://www.cairn.info/revue-cites-2009-3-page-67.htm.
Merzeau (L.), « La présence, plutôt que l'identité », *Documentaliste-Sciences de l'Information* 2010, vol. 47, p. 32, disponible à : https://www.cairn.info/revue-documentaliste-sciences-de-l-information-2010-1-page-32.htm#re6no6.
Michalevsky (Y.), **Schulman** (A.), **Arumugam** (G.), **Boneh** (D.) et **Nakibly** (G.), « Power spy : location tracking using mobile device power analysis », *Security Symposium* 2015, disponible à : https://crypto.stanford.edu/powerspy/files/powerspy.pdf.
Montjoye (Y.-A. de), **Hidalgo** (C.), **Verleysen** (M.) et **Blondel** (V.), « Unique in the Crowd: The privacy bounds of human mobility », *Scientific Reports* 2013, nº 1376, p. 2, disponible à : https://www.nature.com/articles/srep01376.pdf.

Moore (A.), « Defining privacy », *Journal of Social Philosophy* 2008, vol. 39, p. 411, disponible à : https://ssrn.com/abstract=1980849.
Morozov (E.), « The real privacy problem », *MIT Tech Review* 2013, vol. 116, p. 32, disponible à : https://www.technologyreview.com/s/520426/the-real-privacy-problem/.
Nguyen (T.), **Hui** (P.-M.), **Harper** (F.), **Terveen** (L.) et **Konstan** (J.), « Exploring the filter bubble : the effect of using recommender systems on content diversity », *WWW* 2014, p. 677, disponible à : https://www2.kbs.uni-hannover.de/fileadmin/institut/pdf/webscience/2016-17/papers/nej1.pdf.
Nissenbaum (H.), « A contextual approach to privacy online », *Dædalus* 2011, vol. 140, p. 32, disponible à : https://www.amacad.org/sites/default/files/daedalus/downloads/11_fall_nissenbaum.pdf.
Nouwens (M.), **Liccardi** (I.), **Veale** (M.), **Karger** (D.) et **Kagal** (L.), « Dark patterns after the GDPR : scraping consent pop-ups and demonstrating their influence », *CHI'* avr. 20, Honolulu, disponible à : https://arxiv.org/pdf/2001.02479.pdf.
Olejnik (L.), **Castelluccia** (C.) et **Janc** (A.), « Why Johnny can't browse in peace : on the uniqueness of web browsing history patterns », *5th Workshop on Hot Topics in Privacy Enhancing Technologies* 2012, Vigo, disponible à : https://hal.inria.fr/hal-00747841/document.
Ostrom (V.) et **Ostrom** (E.), « Public goods and public choices », in *Alternatives for delivering public services : toward improved performance*, dir. **Savas** (E.), WestviewPress, 1977, p. 7.
Pierrat (E.), « La privatisation de la censure », *Constructif* 2020, nº 56, p. 32, disponible à : https://www.cairn.info/revue-constructif-2020-2-page-32.htm?contenu=article.
Popper (K.), « The moral responsibility of the scientist », *Encounter* mars 1969, p. 53, disponible à : https://www.unz.com/print/Encounter-1969mar-00052/.
Rallet (A.) et **Rochelandet** (F.), « La régulation des données personnelles face au web relationnel : une voie sans issue ? », *Réseaux* 2011, nº 167, p. 40, disponible à : https://www.cairn.info/revue-reseaux-2011-3-page-17.htm.
Schaub (F.), **Baleko** (R.) et **Faith Cranor** (L.), « Designing effective privacy notices and controls », *IEEE Internet Computing* 2017, disponible à : https://ieeexplore.ieee.org/document/7927931.
Schroeder (R.), « Big data and the brave new world of social media research », *Big Data and Society* 2014, disponible à : https://journals.sagepub.com/doi/full/10.1177/2053951714563194.
Shannon (C.), « A mathematical theory of communication », *The Bell System Technical Journal* 1948, vol. 27, p. 379, disponible à : http://pespmc1.vub.ac.be/books/Shannon-TheoryComm.pdf.
Sunstein (C.), « Fifty shades of manipulation », *Journal of Marketing Behavior* 2016, vol. 1, p. 213, disponible à : https://ssrn.com/abstract=2565892.
Sweeney (L.), « Weaving Technology and policy together to maintain confidentiality », *The Journal of Law, Medicine and Ethics* 1997, vol. 25, p. 98.
Thuillier (G.), « À propos de l'affaire des fiches : le maintien du système des fiches de 1905 à 1914 », *Revue administrative* 1997, nº 295, p. 21.
Thuillier (G.), « À propos de l'affaire des fiches. Les mésaventures du préfet Gaston Joliet », *Revue administrative* 1994, nº 278, p. 133.
Thuillier (G.), « Autour d'Anatole France : le capitaine Mollin et l'affaire des fiches en 1904 », *Revue administrative* 1986, nº 234, p. 549.
Tréguer (F.), « US technology companies and State surveillance in the post-Snowden context : between cooperation and resistance », *CERI* 2018, disponible à : https://halshs.archives-ouvertes.fr/halshs-01865140/document.
Utz (C.), **Degeling** (M.), **Fahl** (S.), **Schaub** (F.) et **Holz** (T.), « (Un)informed consent : studying GDPR consent notices in the field », *CCS'* nov. 2019, Londres, disponible à : https://arxiv.org/pdf/1909.02638.pdf.
Whitaker (J.), **Reaves** (B.), **Prasad** (S.) et **Enck** (W.), « Thou shalt discuss security : quantifying the impacts of instructions to RFC authors », *SSR '19* nov. 2019, p. 57.

Zhang (J.), « Operationalizing data quality through data governance », in *Data governance. Creating value from information assets*, dir. **Bhansali** (N.), CRC Press, 2014, p. 66.

§ IV. Rapports, études, avis et communications

Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, *Manuel de droit européen en matière de protection des données 2018*, Luxembourg, Office des publications de l'Union européenne, 2019, disponible à : https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_fr.pdf.
Autorité de la concurrence, *Rapport annuel 2019,* Paris, La Documentation française, disponible à : https://www.autoritedelaconcurrence.fr/sites/default/files/2020-07/rapport-annuel-2019.pdf.
Braibant (G.), « Données personnelles et société de l'information. Rapport au Premier ministre sur la transposition en droit français de la directive n° 95/46 », Paris, La Documentation française, 1998, disponible à : https://www.vie-publique.fr/sites/default/files/rapport/pdf/984000836.pdf.
Cadiet (L.), « L'open data des décisions de justice. Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice. Rapport à la garde des Sceaux », 2017, disponible à : http://www.justice.gouv.fr/publication/open_data_rapport.pdf.
Calais-Auloy (J.) (dir.), « Propositions pour un nouveau droit de la consommation, Rapport de la commission de refonte du droit de la consommation au secrétaire d'État auprès du ministre de l'Économie, des Finances et du Budget chargé du Budget et de la Consommation », Paris, La Documentation Française, 1985.
CEPD, Avis 5/2018, avis préliminaire sur le respect de la vie privée dès la conception, 31 mai 2018, disponible à : https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_fr.pdf.
CEPD, Guidelines 05/2020 on consent under Regulation 2016/679, 4 mai 2020, disponible à : https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
CEPD, Guidelines 4/2019 on article 25. Data protection by design and by default, 13 nov. 2019, disponible à : https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_fr.
CEPD, Lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées, 8 oct. 2019, disponible à : https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_fr.pdf.
CNIL, « À votre écoute. Exploration des enjeux éthiques, techniques et juridiques des assistants vocaux », Livre Blanc, n° 1, 2020, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/cnil_livre-blanc-assistants-vocaux.pdf.
CNIL, « Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle », Rapport de synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une République numérique, déc. 2017, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf.
CNIL, « Premiers éléments d'analyse de la CNIL. Blockchain », sept. 2018, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf.
CNIL, « Vie privée à l'horizon 2020. Paroles d'experts », n° 1, 2010, disponible à : https://linc.cnil.fr/sites/default/files/typo/document/CNIL-CAHIERS_IPn1.pdf.
CNIL, *Rapport d'activité 1978-1980,* Paris, La Documentation française, 1980, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/20171116_rapport_annuel_cnil_-_1er_rapport_dactivite_1978-1980_vd.pdf.

CNIL, *Rapport d'activité 1993,* Paris, La Documentation française, 1994, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/20171116_rapport_annuel_cnil_-_rapport_dactivite_1993_vd.pdf.
CNIL, *Rapport d'activité 2000,* Paris, La Documentation française, 2001, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/20171116_rapport_annuel_cnil_-_rapport_dactivite_2000_vd.pdf.
CNIL, *Rapport d'activité 2002,* Paris, La Documentation française, 2003, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/20171116_rapport_annuel_cnil_-_rapport_dactivite_2002_vd.pdf.
CNIL, *Rapport d'activité 2008,* Paris, La Documentation française, 2009, disponible à : https://www.cnil.fr/sites/default/files/typo/document/CNIL-29erapport_2008.pdf.
CNIL, *Rapport d'activité 2010,* Paris, La Documentation française, 2011, disponible à : https://www.cnil.fr/sites/default/files/typo/document/CNIL_rapport_annuel_ 2010.pdf.
CNIL, *Rapport d'activité 2013,* Paris, La Documentation française, 2014, disponible à : https://www.cnil.fr/sites/default/files/typo/document/CNIL_34e_Rapport_annuel_2013.pdf.
CNIL, *Rapport d'activité 2014,* Paris, La Documentation française, 2015, disponible à : https://www.cnil.fr/sites/default/files/typo/document/CNIL-35e_rapport_annuel_2014.pdf.pdf.
CNIL, *Rapport d'activité 2015,* Paris, La Documentation française, 2016, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/cnil-36e_rapport_annuel_2015_0.pdf.
CNIL, *Rapport d'activité 2016,* Paris, La Documentation française, 2017, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/cnil-37e_rapport_annuel_2016.pdf.
CNIL, *Rapport d'activité 2017,* Paris, La Documentation française, 2018, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/cnil-38e_rapport_annuel_2017.pdf.
CNIL, *Rapport d'activité 2018*, Paris, La Documentation française, 2019, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/cnil-39e_rapport_annuel_2018.pdf.
CNIL, *Rapport d'activité 2019,* Paris, La Documentation française, 2020, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/cnil-40e_rapport_annuel_2019.pdf.
CNIL, *Voix, image et protection des données personnelles*, Paris, La Documentation française, 1996.
Commission des clauses abusives, *Rapport annuel 2018*, Paris, disponible à : http://www.clauses-abusives.fr/wp-content/uploads/2019/06/CCA-Rapport-Annuel-version-definitive.pdf.
Conseil d'État, « Le droit souple », *Rapport Public 2013*, Paris, La Documentation française, 2013, disponible à : https://www.vie-publique.fr/sites/default/files/rapport/pdf/144000280.pdf.
Conseil d'État, « Le numérique et les droits fondamentaux », *Rapport Public 2014*, Paris, La Documentation française, 2014, disponible à : https://www.vie-publique.fr/sites/default/files/rapport/pdf/144000541.pdf.
Conseil d'État, « Les autorités administratives indépendantes », *Rapport Public 2001*, Paris, La Documentation française, 2001, disponible à : https://www.vie-publique.fr/sites/default/files/rapport/pdf/014000275.pdf.
Conseil d'État, « Les conséquences du développement de l'Informatique sur les libertés publiques et privées et sur les décisions administratives », *Rapport Public 1969-1970*, Paris, La Documentation française, 1970.
Conseil de l'Europe, « Rapport explicatif de la Convention 108 », Strasbourg, 28 janv. 1981, disponible à : https://rm.coe.int/16800ca471.
Conseil fédéral suisse, « Message concernant la loi fédérale sur la protection des données (LPD) », 23 mars 1988, *Feuille fédérale,* 140e année, vol. 2, p. 421, disponible à : https://www.amtsdruckschriften.bar.admin.ch/viewOrigDoc.do?id=10105439.
Cour de cassation, « Le juge et la mondialisation dans la jurisprudence de la Cour de cassation », *Étude Annuelle 2017*, Paris, La Documentation française, 2017, disponible à : https://www.courdecassation.fr/IMG/Cour de cassation_Etude 2017.pdf.

Danet (J.), **Grunvald** (S.), **Harzog-Evans** (M.) et **Le Gall** (Y.), *Prescription, amnistie et grâce en France*, Rapport final, Nantes, mars 2006, disponible à : http://www.antoniocasella.eu/archica/Danet_prescription_amnistie_grace_2006.pdf.
Défenseur des droits et CNIL, « Algorithmes : prévenir l'automatisation des discriminations », 2020, disponible à : https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/ddd_algorithmes_access_0.pdf.
Delattre (F.), « Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », Assemblée nationale, nº 1537, 13 avr. 2004, disponible à : http://www.assemblee-nationale.fr/12/pdf/rapports/r1537.pdf.
Department of Justice, *Overview of the Privacy Act of 1974*, 2015, disponible à : https://www.justice.gov/opcl/file/793026/download#page=2&zoom=auto,-169,610.
Détraigne (Y.) et **Escoffier** (A.-M.), « Rapport d'information relatif au respect de la vie privée à l'heure des mémoires numériques », Sénat, nº 441, 27 mai 2009, disponible à : https://www.senat.fr/rap/r08-441/r08-4411.pdf.
Dintilhac (J.-P.) (dir.), « Rapport du groupe de travail chargé d'élaborer une nomenclature des préjudices corporels », juill. 2005, disponible à : https://solidarites-sante.gouv.fr/IMG/pdf/Rapport_groupe_de_travail_nomenclature_des_prejudices_corporels_de_Jean-Pierre_Dintilhac.pdf.
Falque-Pierrotin (I.), « Rapport de la mission interministérielle sur l'Internet. "Internet, enjeux juridiques" », Paris, La Documentation française, 1997, disponible à : https://www.ladocumentationfrancaise.fr/rapports-publics/974057500/index.shtml.
Forteza (P.), « Rapport sur le projet de loi relatif à la protection des données personnelles », Assemblée nationale, nº 592, 25 janv. 2018, disponible à : http://www.assemblee-nationale.fr/15/pdf/rapports/r0592.pdf.
Foyer (J.), « Rapport sur le projet de loi modifié par le Sénat relative à l'informatique et aux fichiers », Assemblée nationale, nº 3352, t. 1, 14 déc. 1977, disponible à : https://www.senat.fr/rap/l77-3352/l77-33521.pdf.
G29, WP 136, Avis 4/2007 du groupe de travail relatif au concept de données à caractère personnel, 20 juin 2007, disponible à : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_fr.pdf.
G29, WP 148, Avis 01/2008 sur les aspects de la protection des données liés aux moteurs de recherche, 4 avr. 2008disponible à : https://www.cnil.fr/sites/default/files/typo/document/wp148_fr.pdf.
G29, WP 171, Avis 02/2010 sur la publicité comportementale en ligne, 22 juin 2010, disponible à : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_fr.pdf.
G29, WP 173, Avis nº 3/2010 sur le principe de responsabilité, 13 juill. 2010, disponible à : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_fr.pdf.
G29, WP 185, Avis 13/2011 sur services de géolocalisation des dispositifs mobiles intelligents, 16 mai 2011, disponible à : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_fr.pdf.
G29, WP 187, Avis 15/2011 relatif à la définition du consentement, 13 juill. 2011, disponible à : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_fr.pdf.
G29, WP 207, Avis 6/2013 sur la réutilisation des informations du secteur public (ISP) et des données ouvertes, 5 juin 2013, disponible à : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_fr.pdf.
G29, WP 216, Avis 5/2014 sur les techniques d'anonymisation, 10 avr. 2014, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/wp216_fr.pdf.
G29, WP 217, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, 9 avr. 2014, disponible à : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf.

G29, WP 243 rév. 01, Lignes directrices concernant les délégués à la protection des données (DPD), 5 avr. 2017, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/wp243rev01_fr.pdf.
G29, WP 244 rév. 01, Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable de traitement ou d'un sous-traitant, 5 avr. 2017, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/wp244rev01_fr.pdf.
G29, WP 248 rév. 01, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est "susceptible d'engendrer un risque élevé" aux fins du règlement (UE) 2016/679, 4 oct. 2017, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf.
G29, WP 251 rév. 01, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, 6 févr. 2018, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/wp251_profilage-fr.pdf.
G29, WP 259 rév. 01, Lignes directrices sur le consentement au sens du règlement 2016/679, 10 avr. 2018, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf.
G29, WP 260 rév. 01, Lignes directrices sur la transparence au sens du règlement 2016/679, 11 avr. 2018, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/wp260_guidelines-transparence-fr.pdf.
G29, WP 37, Document de travail. Le respect de la vie privée sur Internet. Une approche européenne intégrée sur la protection des données en ligne, 21 nov. 2000, disponible à : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp37_fr.pdf.
Gélard (P.), « Rapport sur les autorités administratives indépendantes. Office parlementaire d'évaluation de la législation », Sénat, nº 404, 15 juin 2006, disponible à : https://www.senat.fr/rap/r05-404-2/r05-404-21.pdf.
Genner (S.), « ON / OFF. Risks and rewards of the anytime-anywhere Internet », University of Zurich, 2015, disponible à : https://vdf.ch/on-off-e-book.html.
Gorce (G.) et **Pillet** (F.), « Rapport d'information sur l'open data et la protection de la vie privée », Sénat, nº 469, 16 avr. 2014, disponible à : https://www.senat.fr/rap/r13-469/r13-4691.pdf.
Gouzes (G.), « Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », Assemblée nationale, nº 3526, 9 janv. 2002, disponible à : http://www.assemblee-nationale.fr/11/pdf/rapports/r3526.pdf.
Guinchard (S.), « Rapport au garde des Sceaux. L'ambition raisonnée d'une justice apaisée », Paris, La Documentation française, 2008, disponible à : https://www.vie-publique.fr/rapport/29883-lambition-raisonnee-dune-justice-apaisee.
Hammadi (R.) et **Le Lock** (A.), « Rapport sur le projet de loi relatif à la consommation », Assemblée nationale, nº 1156, 13 juin 2013, disponible à : http://www.assemblee-nationale.fr/14/pdf/rapports/r1156.pdf.
Hyest (J.-J.), **Anziani** (A.), **Borvo Cohen-Seat** (N.), **Colombat** (P.-Y.), **Détraigne** (Y.), **Escoffier** (M.-A.) et **Vial** (J.-P.), « Rapport d'information par le groupe de travail sur les conflits d'intérêts », Sénat, nº 518, 12 mai 2011, disponible à : https://www.senat.fr/rap/r10-518/r10-5181.pdf.
Joissains (S.), « Rapport sur le projet de loi adopté par l'Assemblée nationale après engagement de la procédure accélérée relatif à la protection des données personnelles », Sénat, nº 350, 14 mars 2018, disponible à : https://www.senat.fr/rap/l17-350/l17-3501.pdf.
Lacombe (R.), **Bertin** (P.-H.), **Vauglin** (F.) et **Villefosse** (A.), « Pour une politique ambitieuse des données publiques. Les données publiques au service de l'innovation et de la transparence. Rapport au ministre de l'Industrie de l'Énergie et l'Économie numérique », École des Ponts ParisTech, 2011, disponible à : https://www.vie-publique.fr/sites/default/files/rapport/pdf/114000407.pdf.
Lambert-Faivre (Y.) (dir.), « L'indemnisation du dommage corporel. Rapport au Garde des Sceaux », 22 juill. 2003, disponible à : http://www.justice.gouv.fr/art_pix/syntheseindemcorp.pdf.

Le Dain (A.-Y.) et **Gosselin** (P.), « Rapport d'information sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française », Assemblée nationale, nº 4544, 22 févr. 2017, disponible à : http://www.assemblee-nationale.fr/14/rap-info/i4544.asp#P1140_280381.
Léger (L.) (dir.), *Mes data sont à moi. Pour une patrimonialité des données personnelles*, Génération Libre, janv. 2018, disponible à : https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf.
Leuenberger (M.) et **Meier** (J.), « Évènements survenus au DFJP. Rapport de la commission d'enquête parlementaire », Parlement suisse, nº 89.006, 22 nov. 1989, disponible à : https://www.parlament.ch/centers/documents/fr/ed-berichte-puk-ejpd-f.pdf.
Matras (F.) et **Marleix** (O.), « Rapport d'information sur la déontologie des fonctionnaires et l'encadrement des conflits d'intérêts », Assemblée nationale, nº 611, du 31 janv. 2018, disponible à : http://www.assemblee-nationale.fr/15/pdf/rap-info/i0611.pdf.
Nadler (J.) *et al.*, « Investigation of competition in digital markets. Majority staff report and recommandations », House of Representatives, 2020, disponible à : https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf.
OCDE, « Rapport sur la table ronde sur le recours à l'informatique pour les travaux parlementaires », nº 4312, 23 avr. 1979.
Quénet (M.), « Quel avenir pour les archives de France ? Rapport au premier ministre », Paris, La Documentation française, 2011, disponible à : https://www.vie-publique.fr/rapport/31703-quel-avenir-pour-les-archives-de-france.
Rémond (R.), *Le « fichier juif »* (rapport au Premier ministre), Paris, Plon, 1996.
Supiot (E.) (dir.), « Le procès pénal à l'épreuve de la génétique », Rapport Mission de recherche droit et justice, 2017, disponible à : http://www.gip-recherche-justice.fr/wp-content/uploads/2017/10/14-34-Le-procès-pénal-à-lépreuve-de-la-génétique.pdf.
The United States Digital Service, « Identifying security vulnerabilities in Department of Defense websites – Hack the Pentagon », *Report to Congress* 2016, disponible à : https://www.usds.gov/report-to-congress/2016/hack-the-pentagon/.
Théry (J.-F.) et **Falque-Pierrotin** (I.), « Internet et les réseaux numériques », Conseil d'État, 2 juill. 1998, Paris, La Documentation française, 1998, disponible à : https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/984001519.pdf.
Thyraud (J.), « Rapport sur le projet de loi, adopté par l'Assemblée nationale, relatif à l'informatique et aux libertés », Sénat, nº 72, 10 nov. 1977, disponible à : https://www.senat.fr/rap/l77-072/l77-0721.pdf.
Tricot (B.), « Rapport de la commission Informatique et libertés », Paris, La Documentation française, 1975, disponible à : https://www.cnil.fr/sites/default/files/atoms/files/rapport_tricot_1975_vd.pdf.
Türk (A.), « Rapport sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », Sénat, nº 218, 19 mars 2003, disponible à : https://www.senat.fr/rap/l02-218/l02-2181.pdf.
United States Department of Health, Education and Welfare, « Records, computers, and the rights of citizens », 1973, disponible à : https://www.justice.gov/opcl/docs/rec-com-rights.pdf.
Veil (S.) (dir.), « Redécouvrir le Préambule de la Constitution. Rapport au président de la République », Paris, La Documentation française, déc. 2008, disponible à : https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000758.pdf.
Vichnievsky (L.) et **Gosselin** (P.), « Rapport d'information sur le bilan et les perspectives des actions de groupe », Assemblée nationale, 11 juin 2020, nº 3085, disponible à : http://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b3085_rapport-information.pdf.
Villani (C.) (dir.), « Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne », 28 mars 2018, disponible à : https://www.vie-publique.fr/sites/default/files/rapport/pdf/184000159.pdf.
White House, « Big data : a report on algorithmic systems, opportunity and civil rights », *Executive office of the President* mai 2016, disponible à :

https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.
Zuiderveen Borgesius (F.), « Discrimination, artificial intelligence and algorithmic decision-making », Strasbourg, Conseil de l'Europe 2018, disponible à : https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73.

§ V. Articles d'encyclopédies et dictionnaires

Akoka (J.) et **Comyn-Wattiau** (I.) (dir.), *Encyclopédie de l'informatique et des systèmes d'information*, Vuibert, 2006.
Cornu (G.) (dir.), *Vocabulaire juridique*, 13e éd., Paris, PUF, 2020.
Cornu (M.), **Orsi** (F.) et **Rochfeld** (J.) (dir.), *Dictionnaire des biens communs*, Paris, PUF, 2017.
Dictionnaire de l'Académie française, 9e éd.
Gaffiot (F.), *Dictionnaire Latin-Français*, Hachette, 2000.
Guinchard (S.) et **Debard** (T.) (dir.), *Lexique des termes juridiques*, Dalloz, 2020.
JCl. administratif, fasc. 274-50, « Informatique – Commission nationale de l'informatique et des libertés », par **Perray** (R.), 2019 (actu. 2020).
JCl. civil annexes, Vo Propriété littéraire et artistique, fasc. 1134, « Objet du droit d'auteur. Œuvres protégées. Notion d'œuvre », par **Bensamoun** (A.) et **Goffre** (J.), 2019.
JCl. civil code, art. 16 à 16-4, fasc. 72, « Respect et protection du corps humain. Le mort », par **Beignier** (B.) et **Puyo** (Y.), 2013 (actu. 2017).
JCl. civil code, art. 60, fasc. unique, « Actes de l'état civil. Changement de prénom », par **Marie** (C.), 2017.
JCl. comm., fasc. 34, « Droit au respect de la vie privée. Définition conceptuelle du droit subjectif », par **Saint-Pau** (J.-C.), 2016 (actu. 2019).
JCl. comm., fasc. 930, « Données à caractère personnel. Introduction générale et champ d'application de la règlementation relative à la protection des données personnelles », par **Perray** (R.), 2019 (actu. 2020).
JCl. comm., fasc. 940, « Données à caractère personnel. Obligations des personnes mettant en œuvre des traitements de données à caractère personnel et droits des personnes concernées », par **Perray** (R.), 2016 (actu. 2020).
JCl. comm., fasc. 942, « Le délégué à la protection des données (DPD) », par **Desgens-Pasanau** (G.), 2018.
JCl. entreprise individuelle, fasc. 1932, « Fonds de commerce. Fonds de commerce électronique. Cession », par **Castagné** (S.), 2014 (actu. 2017).
JCP pénal code, fasc. 20, « Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques », par **Mihman** (A.), 2018.
Larousse, *Dictionnaire de Français*.
Le Lamy droit du numérique, *Vo* « Des informations qui ne sont pas disponibles », actu. 2018, dir. **Vivant** (M.).
Le Lamy droit du numérique, *Vo* « Historique de la notion de fichier », actu. 2020, dir. **Vivant** (M.).
Le Lamy droit du numérique, *Vo* « Qu'entend-t-on par données "sensibles" », actu. 2020, dir. **Vivant** (M.).
Littré (É.), *Le nouveau Littré. Le dictionnaire de référence de la langue française*, Garnier, 2007.
Rép. civ. Dalloz, *Vo* « Assurance de personnes : vie – prévoyance », par **Kullmann** (J.), 2013 (actu. 2020).
Rép. civ. Dalloz, *Vo* « Biens », par **Libchaber** (R.), 2016 (actu. 2019).
Rép. civ. Dalloz, *Vo* « Clientèle. Opérations sur la clientèle », par **Barbier** (H.) et **Heinich** (J.), 2016.

Rép. civ. Dalloz, *V°* « Contrat : formation », par **Dissaux** (N.), 2017 (actu. 2020).
Rép. civ. Dalloz, *V°* « Corps humain », par **Penneau** (J.) et **Terrier** (E.), 2019.
Rép. civ. Dalloz, *V°* « Dommages et intérêts », par **Casson** (P.), 2017 (actu. 2020).
Rép. civ. Dalloz, *V°* « État et capacité des personnes – État », par **Gallmeister** (I.), 2016 (actu. 2019).
Rép. civ. Dalloz, *V°* « Inaliénabilité », par **Schütz** (R.-N.), 2014 (actu. 2019).
Rép. civ. Dalloz, *V°* « Nom – Prénom », par **Laroche-Gisserot** (F.), 2014 (actu. 2019).
Rép. civ. Dalloz, *V°* « Personnalité (Droits de la) », par **Lepage** (A.), 2009 (actu. 2020).
Rép. civ. Dalloz, *V°* « Résolution – résiliation », par **Chabas** (C.), oct. 2010 (actu. 2018).
Rép. civ. Dalloz, *V°* « Responsabilité civile environnementale », par **Hautereau-Boutonnet** (M.), 2019 (actu. 2020).
Rép. civ. Dalloz, *V°* « Responsabilité du fait personnel », par **Brun** (P.), 2015 (actu. 2020).
Rép. com. Dalloz, *V°* « Concurrence déloyale », par **Picod** (Y.), **Auguet** (Y.) et **Dorandeu** (N.), 2010 (actu. 2020).
Rép. com. Dalloz, *V°* « Crédit documentaire », par **Stoufflet** (J.), 2004 (actu. 2015).
Rép. com. Dalloz, *V°* « Nom commercial », par **Loiseau** (G.), 2002 (actu. 2011).
Rép. com. Dalloz, *V°* « Transports fluviaux », par **Bailly-Hascoët** (V.), 2003 (actu. 2015).
Rép. cont. adm. Dalloz, *V°* « Autorités de régulation », par **Guillaume** (E.) et **Coudray** (L.), 2010 (actu. 2016).
Rép. cont. adm. Dalloz, *V°* « Communication des documents administratifs », par **Lallet** (A.) et **Nguyen Duy** (P.), 2019.
Rép. cont. adm. Dalloz, *V°* « Jugement », par **Haïm** (V.), 2017 (actu. 2020).
Rép. eur. Dalloz, *V°* « La protection des données personnelles dans les relations internes à l'Union européenne », par **Castets-Renard** (C.), 2018 (actu. 2020).
Rép. eur. Dalloz, *V°* « Télécommunications et communications électroniques », par **Rapp** (L.), 2005 (actu. 2019).
Rép. int. Dalloz, *V°* « Informatique », par **Vivant** (M.) et **Mallet-Poujol** (N.), 2019.
Rép. int. Dalloz, *V°* « Souveraineté », par **Flory** (M.) et **Pancracio** (J.-P.), 2016.
Rép. pén. Dalloz, *V°* « Action civile », par **Ambroise-Castérot** (C.), 2017 (actu. 2020).
Rép. pén. Dalloz, *V°* « Autorités administratives indépendantes », par **Cappello** (A.), 2016 (actu. 2019).
Rép. pén. Dalloz, *V°* « Escroquerie », par **Mascala** (C.), 2016 (actu. 2019).
Rép. pén. Dalloz, *V°* « Prison. Organisation générale. Régime de la détention », par **Céré** (J.-P.), 2015 (actu. 2019).
Rép. proc. civ. Dalloz, *V°* « Action de groupe », par **Ben Hadj Yahia** (S.), 2015 (actu 2019).
Rép. proc. civ. Dalloz, *V°* « Magistrat – Le conflit d'intérêt », par **Balfanti** (L.), 2018 (actu 2019).
Rép. resp. Dalloz, *V°* « Hôpitaux : régimes de responsabilité et de solidarité », par **Grossholz** (C.), 2018 (actu. 2020).
Rép. resp. Dalloz, *V°* « Préjudice réparable », par **Séners** (F.) et **Roussel** (F.), 2019 (actu. 2020).
Rép. resp. Dalloz, *V°* « Responsabilité pénale des personnes publiques : infractions intentionnelles », par **Corioland** (S.), 2019.
Rép. soc. Dalloz, *V°* « Action. Forme des actions », par **Artz** (J.-F.), 2002 (actu. 2019).
Rép. trav. Dalloz, *V°* « Discrimination », par **Lanquetin** (M.-T.), 2010 (actu. 2020).
Rey (A.) et **Rey-Debove** (J.), *Le petit Robert de la langue française*, 2017, Le Robert
Voltaire, *Dictionnaire philosophique*, t. 20, 1878.

TABLE DES ANNEXES

ANNEXE 1 – CONTRÔLES ET SANCTIONS DE LA CNIL

	Contrôles	Avertissements	Mises en demeure	Sanctions pécuniaires	
				Nombre	Montant total
2004	45	7	NR	NR	
2005	104	10	36	NR	
2006	127	4	94	11	168 000 €
2007	164	5	101	9	175 000 €
2008	218	1	126	9	137 100 €
2009	270	4	91	5	75 000 €
2010	308	3	111	5	32 500 €
2011	385	13	65	5	190 000 €
2012	458	9	43	4	16 000 €
2013	414	5	57	7	43 000 €
2014	421	7	62	8	191 001 €
2015	510	7	93	3	65 000 €
2016	430	9	82	4	160 000 €
2017	341	5	79	9	371 000 €
2018	310	1	48	9	1 196 000 €
2019	300	2	42	7	51 370 000 €
Moy.	300	5,75	75	6,8	

Légende :

- NR : non renseigné
- Moy. : moyenne

Source : Rapports d'activité de la CNIL

ANNEXE 2 – DÉNONCIATIONS AU PARQUET EFFECTUÉES PAR LA CNIL

	Dénonciations
1978-1980	0
1980 -1981	0
1981-1982	0
1982-1983	0
1983-1984	1
1985	1
1986	2
1987	2
1988	1
1989	0
1990	0
1991	0
1992	0
1993	1
1994	4
1995	0
1996	0
1997	0
1998	0
1999	2

	Dénonciations
2000	1
2001	1
2002	7
2003	9
2004	2
2005	0
2006	1
2007	5
2008	5
2009	0
2010	1
2011	0
2012	0
2013	0
2014	0
2015	0
2016	0
2017	0
2018	0
2019	0
Total	46

Source : Rapports d'activité de la CNIL

ANNEXE 3 – SÉLECTION DE DÉCISIONS DE PREMIÈRE INSTANCE ET D'APPEL

Les décisions ci-dessous ont été choisies à partir des jugements et arrêts analysés pour établir la nomenclature de préjudices proposée par la présente étude. Seuls les passages les plus pertinents ont été cités.

Une version de cette annexe complétée par d'autres informations est accessible à : https://www.these.vergnolle.org

Décision	Types de préjudice	Réparation allouée
TGI Nanterre, 1re ch., 16 janv. 2002, no 01/03883	« En revanche, le tribunal constate qu'il résulte des écritures de Y Z que celle-ci a été **blessée d'être représentée** comme une femme ayant une liaison avec un homme beaucoup plus jeune qu'elle ».	« Les atteintes subies en l'espèce par Y Z seront indemnisées par la somme de **12 000 euros** (78 714,84 F) versée à titre de dommages et intérêts et par une mesure de publication judiciaire ».
TGI Nanterre, 1re ch., 13 mars 2002, no 01/07193	« Les demandeurs insistent sur le **harcèlement** dont ils seraient victimes de la part de la SA HOLA ».	« Eu égard à leur étendue et à leur nature, les atteintes subies en l'espèce doivent en conséquence être indemnisées par les sommes de : – **4 000 euros** s'agissant de X de A – **3 000 euros** s'agissant de N K de A – **1 000 euros** s'agissant de Y I – **2 000 euros** s'agissant de Z I – **500 euros** s'agissant de H I à titre de dommages et intérêts ».

Décision	Types de préjudice	Réparation allouée
TGI Paris, 17e ch., 12 nov. 2003, no 02/18628	« Attendu que s'il est vrai que les trois attestations produites par Z A, rédigées en des termes identiques et généraux, ne suffisent pas à démontrer l'ampleur du préjudice qu'il invoque, elles contiennent cependant les témoignages de leurs signataires indiquant que son couple a été **perturbé** à la suite de la publication en cause ; Que dès lors qu'aucun élément du dossier ne démontre que la liaison prêtée au demandeur était connue du public avant la parution de l'article litigieux, les photographies et les commentaires publiés par VOICI, révélant sans équivoque qu'il était infidèle, ont pu déterminer son épouse à **engager une procédure de divorce** ».	« Que, compte tenu de l'ensemble de ces éléments, il convient de fixer à **2 500 euros** le montant des dommages-intérêts à allouer au demandeur en réparation du préjudice causé ».
TGI Paris, 17e ch., 24 nov. 2003, no 02/09853	« Attendu que s'il est exact que le nom de Z G-Y n'est pas cité dans l'article et que l'"entourage" ne se limite pas à la famille, le demandeur relève à juste titre que la photographie sur laquelle il figure est la seule qui représente un "proche" de "Marlène", puisque celle-ci apparaît isolément sur les sept autres clichés ; qu'en outre, il produit une attestation de son employeur, E F, qui fait notamment état de l' **"énorme trouble au sein de l'entreprise et de la clientèle"** causé par les "révélations sur la santé de (son) employé… dans le journal (ICI PARIS) et (VOICI)", étant toutefois observé que les répercussions ainsi décrites, qui peuvent apparaître excessives et disproportionnées au regard des seules informations contenues dans l'article de VOICI, proviennent également des "révélations" faites par ICI PARIS ».	« Attendu que dans ces conditions, le préjudice résultant pour Z G-Y de la violation de son droit à l'image sera justement réparé par l'allocation de la somme de **1 500 euros** à titre de dommages-intérêts ».

Décision	Types de préjudice	Réparation allouée
TGI Nanterre, 1re ch., 1 mars 2004, no 03/00644	« Attendu que si le principe de la liberté d'information conduit à limiter la portée du droit à l'image en certaines circonstances touchant à l'actualité, la publication de photographies isolant la demanderesse – assise en raison de son état de grossesse avancée – de l'assemblée formée par les policiers, les familles et les proches participant aux obsèques nationales des deux policiers tués dont l'un d'eux était son compagnon, ne saurait être légitime pour "traduire l'indicible et répondre à l'émotion populaire", ni "salutaire pour sensibiliser et cristalliser la mémoire de l'opinion et des autorités sur le drame et ses causes afin que cela ne se reproduise plus à l'avenir" ainsi que l'écrit la société éditrice, alors qu'elle **arrache à son insu l'intéressée à son anonymat** pour en faire complaisamment l'élément central de la manifestation à seule fin de satisfaire l'appétit du public, au mépris de la pudeur, de la retenue et de la sensibilité de la jeune femme dont la douleur est redoublée par cette exposition intempestive qui caractérise la recherche du sensationnel ».	« Attendu que cette publication fautive a causé à X Z qui ne saurait se voir opposer un délai qui résulte de la résistance de l'éditeur, un préjudice moral qui sera réparé par l'allocation de la somme de **10 000 euros** à laquelle le tribunal l'évalue sans qu'il y ait lieu à une mesure complémentaire de publication forcée ».
TGI Paris, 17e ch., 6 avr. 2005, no 04/05663	« Mais attendu que Y A se plaint à juste titre de **la traque** dont elle a été l'objet, alors qu'elle croyait pouvoir partager, à l'abri de toute indiscrétion, des moments d'intimité qui se trouvent en définitive divulgués à des milliers de lecteurs, sur la page de couverture de surcroît ; que deux attestations versées aux débats témoignent à cet égard du caractère quasi inaccessible de la propriété de la demanderesse en Corse, ainsi que du contrecoup qui en est résulté pour elle ; (…) Attendu que le tribunal se doit de tenir compte de la réitération des atteintes portées à la vie privée de l'artiste qui **traduisent un acharnement et un harcèlement** à son encontre ».	« Attendu qu'une indemnité de **12 000 euros** apparaît dans ces conditions de nature à réparer le préjudice subi par la demanderesse ».

Décision	Types de préjudice	Réparation allouée
TGI Paris, 17e ch., 2 nov. 2005, no 04/16614	« Attendu que la demanderesse qui n'avait aucune vocation à voir des photographies prises au téléobjectif la représentant publiées sans son autorisation, sur une pleine page d'un magazine à très fort tirage qui se présente comme "Le féminin people du lundi", a subi du fait de cette publication illicite de son image **une atteinte à son anonymat** ».	« Préjudice qu'il convient, en l'espèce, de réparer par l'allocation d'une somme de **3 000 euros** ».
TGI Nanterre, réf., 27 janv. 2006, no 06/00086	« Attendu que ces atteintes ouvrent donc droit à réparation du préjudice non sérieusement contestable en son principe ni même en son montant, qui sera apprécié en prenant en considération d'une part, le contenu indiscret de l'article qui expose à la curiosité suscitée d'un très large lectorat les activités privées de la demanderesse ainsi que ses sentiments réels ou supposés les plus intimes, d'autre part, le nombre et la nature des clichés réalisés selon un procédé déloyal, mais également **la surveillance de l'intéressée, qui la prive ainsi de toute liberté d'aller et de venir** constituant l'une des prérogatives du droit à la vie privée de valeur égale à la liberté d'expression ».	« Qu'il lui sera alloué la somme de **6 000 euros** à titre de provision indemnitaire ».
TGI Aix-en-Provence, 25 avr. 2006 no 06/00464	« En l'espèce l'évocation sur un média, tel que l'internet, des circonstances de la mort de Z-N X et des conditions dans lesquelles G H a été reconnu coupable de l'enlèvement et de l'assassinat sont d'évidence de nature à **raviver l'immense douleur** des proches de la victime. Si la douleur ainsi ravivée a pu dans certaines hypothèses être considérée comme constituant une atteinte à la vie privée digne de protection, il n'en est pas ainsi comme en l'espèce où les faits évoqués remontent à trente années et relèvent de l'histoire judiciaire de la France compte tenu de l'exécution de G H ».	« Il convient en conséquence de considérer que C X, Z-N O épouse X, A X, D X et B X épouse Y ne démontrent pas l'existence d'une atteinte à l'intimité de leur vie privée justifiant l'intervention du juge des référés ».

Décision	Types de préjudice	Réparation allouée
TGI Nanterre, réf., 30 juin 2006, nº 06/01542	« Attendu que l'éditeur n'est pas fondé à tirer argument des thèmes intimes traités dans les chansons pour écarter le préjudice ressenti par l'artiste, laquelle ne renonce nullement à la protection de son intimité ; que les déclarations d'Anggun A en des termes contrôlés et anodins sur ses liens sentimentaux avec son mari, son goût des belles robes et ses activités ancillaires notamment, livrées en des termes elliptiques, contrôlés et convenus à l'occasion d'interviews à vocation essentiellement promotionnelle ne sauraient pas plus minimiser le préjudice allégué, qui résulte du **trouble né de la dépossession de leurs sentiments et de leur intimité** que ressentent les plaignants ».	« Attendu dans ces circonstances qu'il sera alloué à titre de provision indemnitaire la somme de **10 000 euros** à chacun des plaignants sans qu'il y ait lieu à une mesure de publication ».
TGI Nanterre, 1re ch., 26 oct. 2006, nº 06/06902	« Le préjudice moral est aggravé par la **traque subie** par celle-ci qui se déduit de **la surveillance** dont elle fait l'objet, du mode de prise de vue qui étaient nécessairement connues de la société Prisma Presse et de la persistance du journal à violer délibérément ses droits ».	« Il sera donc alloué à Y Z une indemnité d'un montant de **2 500 euros** en réparation du préjudice subi par la publication de l'édition nº 662 et de **6 000 euros** en réparation du préjudice subi par la publication de l'édition nº 663 ».

Décision	Types de préjudice	Réparation allouée
TGI Nanterre, réf., 18 sept. 2006, nº 06/02105	« Attendu que le préjudice résultant de ces atteintes ouvre droit à une créance indemnitaire non contestable en son principe, dont le montant est apprécié en prenant en considération d'une part, les éléments factuels qu'invoque les plaignants, le contenu indiscret et racoleur de l'article qui expose la vie sentimentale passée et présente, réelle ou supposée, des intéressés présentés de surcroît dans des moments de loisirs et dans des scènes de tendresse, sans aucune nécessité d'information, à la curiosité suscitée d'un large lectorat à seule fin de le divertir le nombre, la nature intime et complice de certains clichés réalisés clandestinement à la faveur d'une **surveillance**, d'autre part la persistance de l'éditeur à méconnaître les droits fondamentaux du demandeur malgré quatre précédentes condamnations prononcées à son encontre pour des faits similaires, créant **un sentiment d'impuissance** ; Attendu que si B C peut légitimement ressentir douloureusement l'étalage racoleur de sa relation amoureuse, sa crainte de voir compromises ses **relations professionnelles** avec G H reste cependant hypothétique ».	« Attendu qu'il sera alloué dans ces conditions à Z A la somme provisionnelle de **9000 euros** à titre de dommages et intérêts, propre à compenser le dommage subi ; Pour les relations professionnelles : qu'il lui sera alloué dans ces conditions une provision indemnitaire de **6 000 euros** ».
TGI Nanterre, réf., 22 sept. 2006, nº 06/01949	« Attendu qu'ainsi privés d'une **légitime espérance de tranquillité,** les plaignants subissent un préjudice non sérieusement contestable en son principe, qui doit être apprécié en prenant en considération le contenu indiscret de l'article, le nombre des clichés fixant des poses banales, et la **surveillance** dont les intéressés ont été l'objet ».	« Qu'il sera dès lors alloué à chacun des demandeurs la somme de **7 000 euros** à titre de provision indemnitaire, sans qu'il y ait lieu à une mesure de publication forcée ».
TGI Paris, 17e ch., 30 mai 2007, nº 06/10820	« Les cinq photographies d'illustration prises au téléobjectif, à l'insu du demandeur, établissent, de la part de la société défenderesse, la mise en œuvre d'une **surveillance** incompatible avec le respect de la vie privée à laquelle tout individu peut légitimement prétendre ».	« Attendu que pour l'ensemble de ces motifs, le préjudice moral subi par Z A du fait des atteintes dont il a été victime sera justement réparé par l'allocation de la somme de **6 000 euros** à titre de dommages et intérêts et par une mesure de publication judiciaire, suivant les termes et modalités ci-après fixés dans le dispositif, sans qu'il soit nécessaire d'assortir cette mesure d'une astreinte ».

Décision	Types de préjudice	Réparation allouée
TGI Paris, 17e ch., 30 mai 2007, nº 05/17887	« Que c'est à juste titre que les demandeurs pour l'évaluation de leur préjudice se prévalent du **harcèlement** dont ils font l'objet, grâce à l'emploi des moyens techniques sophistiqués ».	« Qu'il y a lieu en conséquence d'allouer la somme de **1 500 euros** à chacun des demandeurs à titre de dommages et intérêts ».
TGI Paris, 17e ch., 4 juin 2007, nº 06/15541	« Celle-ci produit un certificat médical du 9 mai 2006, faisant notamment état de **signes d'anxiété** en rapport avec l'annonce prématurée dans la presse de son état de grossesse, ce qui apparaît donc moins pertinent plusieurs mois après ».	« Attendu que compte tenu de l'ensemble de ces éléments, il convient d'accorder à la demanderesse la somme de **2 000 euros** à titre de dommages-intérêts en réparation du préjudice subi à la suite des atteintes portées à sa vie privée et à son droit à l'image dans le magazine VOICI, sans qu'une mesure de publication judiciaire n'apparaisse toutefois nécessaire ».
TGI Paris, 17e ch., 4 juin 2007, nº 06/14542	« Attendu qu'il y a lieu en l'espèce de retenir que les intéressés ont été photographiés avec un téléobjectif, ce qui démontre une **surveillance** préjudiciable de leurs activités de loisirs ».	« Attendu que compte tenu de l'ensemble de ces éléments, il convient d'accorder à la demanderesse la somme de **500 euros** et **un euro** au demandeur, à titre de dommages-intérêts en réparation du préjudice subi en France ».
TGI Paris, 17e ch., 11 juill. 2007, nº 06/13598	« Attendu qu'à ce titre il convient, de rappeler une nouvelle fois, que la liberté de la presse ne saurait justifier aucunement, en dehors de toute actualité et légitimité d'informer, **d'épier**, à leur insu, les faits et gestes des demandeurs, lors d'activités strictement privées, à des fins exclusivement mercantiles »	« Attendu qu'au regard de ces éléments d'appréciation, il convient d'allouer à chacun des demandeurs la somme de **1 000 euros** à titre d'indemnisation du préjudice moral subi par eux ».
TGI Paris, 17e ch., 11 juin 2008, nº 07/11090	« Attendu que si la seule constatation de l'atteinte à la vie privée engendre un préjudice dont le principe est acquis, il importe de prendre plus particulièrement en considération la **nature des informations publiées** en l'espèce et qui tendent à révéler une relation adultérine qu'entretiendrait la demanderesse, révélation qui ne peut être que particulièrement néfaste pour elle, même s'il est justifié qu'elle n'a pas toujours été exempte d'une certaine complaisance vis à vis des médias ».	« Qu'il y a lieu en conséquence d'allouer à Y X la somme de **10 000 euros** à titre de dommages et intérêts ainsi qu'une mesure de publication judiciaire, en réparation du préjudice moral qu'elle a subi ».

Décision	Types de préjudice	Réparation allouée
TGI Paris, 17e ch., 12 sept. 2007, no 06/10844	« Attendu qu'il y a lieu en l'espèce de retenir que les intéressés ont été photographiés avec un téléobjectif, ce qui démontre **une surveillance** préjudiciable de leurs activités ; qu'il sera cependant observé à cet égard que les communiqués et mises en demeure versés aux débats n'ont pas été envoyés à la société défenderesse ; que le seul jugement de condamnation produit en ce qui la concerne remonte au 20 décembre 2000 ; que l'audition d'B C par un juge d'instruction, faisant état de sa **souffrance face à ce harcèlement**, date également de l'année 2000 ».	« Attendu que compte tenu de l'ensemble de ces éléments, il convient d'accorder à chacun des demandeurs la somme de **500 euros**, à titre de dommages-intérêts en réparation du préjudice subi en France à la suite des atteintes portées à leur vie privée et à leur droit à l'image dans le numéro 878 du magazine HELLO! ».
TGI Nanterre, 1re ch., 15 mai 2008, no 07/10721	« Ces attestations ainsi que le certificat médical faisant état d'un **état d'anxiété, de tristesse et de ruminations**, établissent suffisamment que dans les semaines ayant suivi la parution de l'article, Y Z s'est trouvée fortement perturbée ».	« Ainsi compte tenu de ces éléments, du caractère indiscret des photographies représentant notamment les intéressés en train de s'embrasser et de la grande diffusion du magazine, il sera alloué à Y Z la somme de **10 000 euros** à titre de dommages-intérêts. Il y a lieu en outre d'interdire toute nouvelle publication des photographies litigieuses dès lors qu'il apparaît que la seule connaissance par la société Prisma presse du caractère illicite de la captation et de la publication des clichés ne suffit pas à la dissuader de les reproduire ».

Décision	Types de préjudice	Réparation allouée
TGI Paris, 17e ch., 9 juill. 2008, no 07/13908	« Attendu qu'il y a lieu, en l'espèce, de retenir comme facteurs aggravant le dommage : – que le magazine HOLA a consacré une place particulièrement importante à ce sujet, à savoir la plus grande partie de la couverture et six pleines pages intérieures ; – que de nombreuses photographies, prises au téléobjectif et fortement agrandies, ont été publiées, surprenant les intéressés dans des moments de nature privée, tendre et intime ; – que même si elles n'ont pas été réalisées par des photographes de la société défenderesse, ces images montrent que la demanderesse **a fait l'objet d'une surveillance**, si ce n'est du **harcèlement** invoqué, préjudiciable à la **tranquillité** à laquelle chacun peut légitimement aspirer ».	« Attendu que compte tenu de l'ensemble de ces éléments, il convient d'accorder à la demanderesse la somme de **800 euros**, à titre de dommages et intérêts en réparation du préjudice subi en France à la suite des atteintes portées à sa vie privée et à son droit à l'image dans le magazine HOLA ».
TGI Paris, 17e ch., 3 nov. 2008, no 07/15835	« Attendu que si la prise de cliché au téléobjectif révèle une **surveillance** préjudiciable au cours d'activités privées de loisirs, il y a lieu, en revanche et en l'espèce, de retenir comme éléments de nature à réduire le préjudice qu'une seule photographie de la demanderesse figure en page intérieure d'un magazine à la diffusion très limitée en France et qu'elle ne révèle rien de particulièrement intime en ce qui la concerne ».	« Attendu que compte tenu de l'ensemble de ces éléments, il convient d'accorder à la demanderesse **un euro**, à titre de dommages et intérêts en réparation du préjudice subi en France à la suite des atteintes portées à sa vie privée et à son droit à l'image dans le magazine CHI No 21 ».
TGI Paris, 17e ch., 12 nov. 2008, no 08/03068	« Que la société Z A ASSOCIES sera également condamnée à verser à F G-X, qui n'est pas connu du grand public et aspire légitimement à la **tranquillité** de sa vie privée ».	« La somme de **5 000 euros** en réparation de son dommage ».
TGI Paris, 17e ch., 12 janv. 2009, no 07/15831	« Attendu que la réalisation de ces nombreux clichés au téléobjectif révèle une **surveillance** préjudiciable au cours d'activités privées de loisirs ».	« Attendu que compte tenu de l'ensemble de ces éléments, il convient d'accorder à la demanderesse la somme de **1 500 euros**, à titre de dommages et intérêts en réparation du préjudice subi en France à la suite des atteintes portées à sa vie privée et à son droit à l'image dans le magazine BUNTE No 24 ».

Décision	Types de préjudice	Réparation allouée
TGI Marseille, réf., 20 mai 2009, nº 09/01163	« Que compte-tenu de ce que le cliché pris à l'insu de Mlle Y a révélé au grand public un état de grossesse que cette dernière avait jusqu'alors légitimement **souhaité vivre intimement et sereinement** ».	« La provision à valoir sur l'indemnisation du préjudice patrimonial et moral peut être fixée à la somme de **10 000 euros** ».
TGI Marseille, 1re ch., 2 juin 2009, nº 07/11509	« Si l'attestation de mademoiselle KRYSTAK est dépourvue de force probante (...), et ne permet pas d'affirmer que monsieur X a dû renoncer à son mariage du fait de la publication, il n'en demeure pas moins que la diffusion du cliché à un large public a eu manifestement des **répercussions sur la vie affective et sociale de l'intéressé** ».	« Il convient de fixer à la somme de **2 000 euros**, et ce y compris la provision allouée en référé, le montant des dommages-intérêts en réparation des conséquences préjudiciables desdites répercussions ».
TGI Nanterre, réf., 12 mars 2010, nº 10/00482	« Attendu qu'en l'espèce pour apprécier l'étendue du préjudice moral indubitablement subi par les demandeurs il y a lieu de prendre en compte : – le nombre de clichés qui illustrent l'article dont un est publié en page de couverture ce qui en majore l'exposition notamment aux usagers des kiosques à journaux, – le fait que cet article **tire Madame X brutalement de l'anonymat**, alors que son exposition médiatique antérieure n'est pas plus alléguée que démontrée, – la discrétion habituelle de Y X, qui ne met pas en scène sa vie privée ».	« Attendu dans ces conditions qu'il y a lieu de leur allouer : – à Madame X une indemnité provisionnelle de **6 000 euros** – à Monsieur X une indemnité provisionnelle de **5 000 euros** sans que les circonstances de la cause justifient la publication d'un communiqué judiciaire qui, deux mois après la publication en cause, aurait pour effet de les exposer plus encore, allant à l'encontre du souci de discrétion mis en avant ».
TGI Nanterre, 1re ch., 8 avr. 2010, nº 09/10123	« Y Z justifie avoir, à plusieurs reprises, exercé des poursuites à l'encontre des magazines édités par A B G et même si la condamnation à des dommages et intérêts doit réparer le dommage ponctuellement réalisé, la réitération des atteintes est de nature à aggraver le ressenti par la demanderesse de cette nouvelle publication, qui marque une forme d'**acharnement** à l'endroit de sa personne ».	« De l'ensemble de ces éléments, il résulte que les prétentions indemnitaires d'Y Z devront être minorées et que son préjudice sera justement indemnisé par la condamnation d'A B G à lui payer la somme de **4 000 euros**, à titre de dommages et intérêts. Il sera également fait droit à la demande d'interdiction de nouvelle publication des photographies litigieuses, intrinsèquement ».

Décision	Types de préjudice	Réparation allouée
TGI Paris, réf., 14 sept. 2010, nº 10/57095	« Par ailleurs, il y a lieu en l'espèce de retenir que les intéressés ont été photographiés avec un téléobjectif – en tout cas à leur insu –, ce qui démontre une **surveillance** préjudiciable de leurs activités de loisirs, alors qu'ils pouvaient se croire à l'abri du regard d'autrui dans un lieu particulièrement discret – rien ne permettant de démentir les explications fournies à cet égard en demande –, ce qui participe à un phénomène de **harcèlement**. De même, les détails fournis dans l'article sur l'itinéraire exact et les conditions d'organisation de la croisière, comme sur les escales à terre, montrent que le **couple a été épié**, ce qui accroît le **sentiment d'impuissance et de dépossession** de toute intimité ».	« En conséquence et compte tenu de l'ensemble des éléments du dossier, comme des déclarations de la demanderesse à l'audience, il convient d'accorder à A Z une provision de **8 000 euros** à valoir sur l'indemnisation de C préjudice et d'ordonner une mesure de publication judiciaire en page de sommaire du magazine CLOSER, sans qu'il soit nécessaire de l'assortir de l'astreinte sollicitée ».
TGI Nanterre, 1re ch., 5 mai 2011, nº 10/10082	« Cette publication est intervenue malgré la volonté de la demanderesse de protéger, y compris judiciairement, ses droits de la personnalité, ce qui est de nature à créer le **sentiment d'impuissance** dont elle fait état ».	« Le préjudice moral subi par Z E sera intégralement réparé, compte tenu de ces éléments, par la condamnation de la société HOLA à lui payer **500 euros** de dommages et intérêts ».
TGI Nanterre, 1re ch., 19 mai 2011, nº 10/11475	« Du fait de l'annonce racoleuse en page de couverture, de la nature des nombreuses photographies réalisées à l'insu des intéressés et fixant ainsi l'image de X Y enceinte, sans son consentement, du **harcèlement** dont sont victimes les demandeurs de la part de la SNC PRISMA PRESSE, en dépit des nombreuses procédures judiciaires initiées par eux à son encontre, la SNC PRISMA PRESSE ne peut sérieusement prétendre à l'absence de tout dommage causé par la publication en cause ».	« Dans ces conditions, l'allocation à X Y de la somme de **5 000 euros** et à Z A de la somme de **3 000 euros** à titre de dommages et intérêts est proportionnée au dommage subi, sans que la mesure de publication forcée sollicitée soit justifiée ».

Décision	Types de préjudice	Réparation allouée
TGI Paris, 17e ch., 7 sept. 2011, nº 10/13204	« Le nombre et la nature des clichés publiés manifestent en outre une indifférence absolue au respect des droits de la demanderesse qui peut souhaiter légitimement, en dépit de la grande notoriété de son compagnon à laquelle elle est conduite à consentir, aspirer à une **forme de tranquillité** dans certaines circonstances, telles que des vacances à la plage. Enfin, une telle publication révèle que la demanderesse et son compagnon ont fait l'objet d'une **surveillance à leur insu** dans un moment de tranquillité, ce qui est de nature à aggraver le préjudice qui en est éprouvé ».	« Au regard de l'ensemble de ces observations, le préjudice résultant pour X Y des atteintes imputables à la société défenderesse, sera justement réparé par l'allocation d'une somme de **8 000 euros** à titre de dommages et intérêts ».
TGI Nanterre, 1re ch., 24 nov. 2011, nº 10/13341	« Ces publications sont donc de nature à aggraver le **sentiment de dépossession** du demandeur, qui justifie au moyen des décisions judiciaires produites de l'attachement qu'il porte au respect de ses droits de la personnalité ».	« Ce préjudice sera intégralement réparé par la condamnation de la société Arnoldo à lui payer **1 000 euros** de dommages et intérêts ».
TGI Nanterre, 1re ch., 19 janv. 2012, nº 11/03759	« Les photographies publiées ont été manifestement prises à l'insu de ce dernier, avivant le **sentiment de traque** dont il fait état ».	« B C de X justifie en revanche, au regard des éléments exposés ci-dessus, d'un préjudice moral qui sera évalué à **1 000 euros** ».
TGI Toulouse, 4e ch., 13 nov. 2012, nº 12/02021	« Cependant, la taille de la photographie, le choix de la placer en couverture, la mention de détails douloureux, destinés à favoriser une curiosité malsaine, constitue un détournement de l'objectif d'information, dans un évident but mercantile, incompatible avec le respect de l'indicible **douleur des proches**, de nature à majorer le **sentiment d'affliction** des parents, qui décrivent bien l'affront fait à leur douleur, que de "revoir le portrait de leur fille O en affiche sur les kiosques, en Une des magazines, dans les mains des passants, puis, une fois le périodique lu, jeté au sol ou dans les poubelles", et ce seulement 10 jours après le décès de l'enfant ».	« Ce préjudice sera réparé par l'octroi de la somme de **6 000 euros** allouée à chacun des parents ».

Décision	Types de préjudice	Réparation allouée
CA Versailles, 10 janv. 2013, nº 11/03192	« Le préjudice de Y D, d'Ernst D et de Z H, d'ordre moral, résulte de ce que sont **exposées** contre leur volonté, aux yeux des lecteurs, des activités strictement privées ou que leur sont prêtés des sentiments qui relèvent de la sphère intime d'un couple ».	« Il convient de porter la condamnation prononcée par les premiers juges aux sommes suivantes : – **2 000 euros** pour Y D, – **1 500 euros** pour Ernst D, – **1 000 euros** pour Z H ».
CA Aix-en-Provence, 12 juin 2014, nº 13/20737	« Que pour parfaitement concevable que soit le choix du journaliste d'aborder le sujet sous un angle critique, constitue une atteinte à la vie privée, à l'image, à la dignité humaine, l'utilisation des pleurs d'une jeune enfant, parfaitement identifiable faute d'image floutée, et le choix de la SA METROPOLE DIFFUSION de les diffuser au mépris du vécu de l'enfant au moment de la diffusion et postérieurement, de sa capacité à assumer les suites d'un événement sur lequel elle n'a plus aucune prise, du sentiment qu'elle aura peut-être **d'avoir été trompée** sur le sens de son intervention, de la **honte** qui peut être la sienne en découvrant la véritable dimension de ce qui n'était que la réaction innocente et spontanée d'une petite fille qui croyait seulement exprimer son affection à l'égard des femmes de service ».	« Que le jugement déféré sera en conséquence infirmé en toutes ses dispositions et statuant à nouveau, la SA METROPOLE DIFFUSION sera condamnée à verser aux époux X, en qualité de représentants légaux de leur fille mineure E, une somme de **5 000 euros** à titre de dommages-intérêts en réparation du préjudice moral causé à l'enfant mineure ».
TGI Paris, réf., 24 nov. 2014, nº 14/59928	« Cette immixtion particulièrement prononcée et insistante dans la vie privée de la demanderesse, qui plus est au moyen de procédés déloyaux, et l'atteinte aux droits de la personnalité qui en résulte, sont la cause d'une **angoisse** et d'un **désarroi** légitimes de la part de Mme X. De plus, une exposition en page de couverture, ainsi que la multiplication des publications, a pour nécessaire conséquence d'aggraver le préjudice moral de Mme X, l'intéressée ayant le **sentiment qu'elle ne peut endiguer cette intrusion incessante** malgré les actions judiciaires entreprises, ce qui peut être la source d'une **anxiété** durable ».	« En conséquence, il convient d'allouer une provision de **12 000 euros** à valoir sur la réparation du préjudice moral que Mme Z X subit. En raison de la nature et l'importance de l'atteinte causée par la société Mondadori Magazine malgré la mise en demeure précédemment reçue et les condamnations déjà intervenues, il convient de faire droit à la demande de publication judiciaire, selon les modalités fixées au dispositif ».

Décision	Types de préjudice	Réparation allouée
TGI Nanterre, 1re ch., 9 avr. 2015, no 13/11685	« Si les clichés litigieux ne comportent aucune image de nature à dévaloriser l'image de la demanderesse et ne dévoilent aucune scène intime, les photographies ayant été prises sur la voie publique, les faits n'en sont pas pour autant négligeables dès lors qu'ils révèlent que Mme X a fait l'objet d'une **surveillance intrusive** par un ou plusieurs photographes ».	« Compte tenu de l'ensemble de ces éléments, il y a lieu d'allouer à Mme X la somme de **3 500 euros** à titre de dommages-intérêts en réparation du préjudice subi à la suite des atteintes portées à sa vie privée et à son droit à l'image par la commercialisation des clichés litigieux par la société défenderesse ».
TGI Nanterre, 1re ch., 24 nov. 2016, no 16/10353	« Il convient également de relever que les attestations produites au débat de Mme C D, maquilleuse présente sur le plateau de tournage de l'émission "Zone interdite" le jour de la parution de l'article poursuivi selon laquelle Mme Y était **bouleversée et choquée**, et des frères de la demanderesse MM. Z et E Y, ce dernier précisant que la demanderesse, issue d'une famille de culture mormone, était **inconsolable et honteuse** au moment de la découverte de la publication litigieuse, témoignent de l'impact de l'article sur Mme Y qui a été **particulièrement affectée** par celui-ci ainsi que par les réactions de certains lecteurs du magazine qui lui ont adressé des correspondances inquiétantes ».	« Compte tenu de l'ensemble de ces éléments, la demanderesse ne justifie pas de l'importance du préjudice moral par elle subi à la hauteur de ses prétentions indemnitaires, lequel sera suffisamment réparé par l'allocation de la somme de **10 000 euros**, sans qu'il soit besoin d'accueillir la demande de publication judiciaire à titre de mesure de réparation complémentaire, cette demande n'étant ni justifiée ni proportionnée en l'espèce ».

Décision	Types de préjudice	Réparation allouée
TGI Nanterre, réf., 13 déc. 2016, nº 16/02457	« La réitération des atteintes et ce malgré les mises en demeure adressées et les condamnations intervenues contre le même magazine qui avait déjà été à l'origine de la révélation exclusive d'une précédente relation sentimentale de l'intéressée en juillet 2015, suscitant un **sentiment d'impuissance** à obtenir le respect de sa vie privée, sont d'autant d'éléments qui aggravent son préjudice. L'attestation rédigée par une des plus proches amies de Mme X datée de septembre 2016 témoigne concrètement de l'**abattement** de Mme X lorsqu'elle a appris, alors qu'elle était en vacances, la parution de l'article dans le magazine Voici révélant sa relation sentimentale, et du **sentiment d'impuissance** consécutif à cette publication puisque Mme X déclarait que la précédente poursuite contre le magazine Voici qui avait révélé sa relation sentimentale avec B C n'avait servi à rien, la précision apportée par son amie selon laquelle "son moral était déjà au plus bas car elle avait appris quelques heures plus tôt l'existence du magazine Public" ne venant pas contredire le retentissement particulier de la parution du magazine Voici ».	Dans ces circonstances, il convient d'allouer à la demanderesse une indemnité provisionnelle de **8 000 euros** à valoir sur la réparation de son préjudice moral au titre de l'article paru dans le magazine Voici nº 1494.
CA Colmar, 9 avr. 2018, nº 16/06017	« Enfin, les consorts Y ne peuvent opposer qu'ils ont déjà une vue directe de l'étage de leur habitation sur la piscine X dès lors qu'il y a une nette différence dans la gradation des préjudices entre être simplement aperçu d'une habitation et **être filmé en continu** sur un support vidéo susceptible de conservation ».	« Il suit de ces énonciations que la décision sera infirmée partiellement en ce qu'elle a rejeté la demande de suppression formée par les époux X en ce qui concerne la caméra Nord ».

ANNEXE 4 – NOMENCLATURE DES PRÉJUDICES EXTRAPATRIMONIAUX

Préjudice émotionnel	Préjudice d'exposition	Préjudice de pistage	Préjudice réputationnel
Affliction	Troubles sur :	Sentiments de :	Atteintes à :
Anxiété	- l'anonymat	- acharnement	- la dignité
Désarroi	- la tranquillité	- dépossession	- l'honneur
Douleur	- la vie affective	- harcèlement	- l'image renvoyée au public
Honte	- la vie sociale	- impuissance	- la réputation
Perturbation		- se sentir sous surveillance	
Rumination		- traque	
Tristesse			

INDEX

(les numéros renvoient aux numéros des paragraphes)

- D -

- E -

- F -

- G -

- H -

- I -

- J -

- L -

- M -

- N -

- R -

- S -

- T -

- V -

- W -

- Y -

TABLE DES MATIÈRES

L’effectivité de la protection des personnes par le droit des données à caractère personnel

Généralement présenté comme une matière réservée aux initiés, le droit des données à caractère personnel intéresse pourtant le plus grand nombre. Les technologies de l’information sont si répandues que les menaces liées à leurs usages pèsent sur tous. L’effectivité de la protection des personnes se révèle être l’enjeu majeur de ce droit.

Pour endiguer les risques d’atteinte aux personnes, le domaine des données à caractère personnel s’est étendu. Pouvons-nous considérer que cette expansion, façonnée au fil des interprétations et modifications législatives, débouche sur une meilleure protection des personnes ? Cela n’est pas certain. Pour parvenir à cette fin, il a été jugé opportun d’encadrer la notion de donnée à caractère personnel. Cette qualification doit être limitée aux données directement identifiantes et aux données indirectement identifiantes dont le traitement induit un lien avec une personne physique. Cette approche a appelé un renforcement du régime juridique associé.

Les règles actuelles de cette matière, bien que nombreuses et enchevêtrées, sont favorables à la mise en œuvre des traitements et les atteintes à la liberté d’autodétermination sont peu encadrées. Afin de prévenir les risques d’atteinte aux personnes, un raffermissement de certains principes a été proposé. C’est surtout une meilleure mise en œuvre de ce droit qu’il a fallu garantir. Celle-ci passe par une intensification et une diversification des contrôles. Elle se matérialise surtout par une amélioration de la réalisation juridictionnelle du droit des données à caractère personnel, qui doit reconnaître aux personnes des moyens effectifs pour agir et défendre leurs données.

On the Effectiveness of Protecting Individuals’ Rights by Data Protection Law

Often presented as a subject matter reserved to experts, data protection law is of interest to many. Over the past couple of decades, Information Technology has become so ubiquitous that threats induced by its use now expose everyone. The effectiveness of protecting individuals’ rights has therefore become the major challenge of data protection law.

The scope of data protection law has expanded over the years in order to adapt to new risks that are continuously arising from the digital society. Has such expansion, shaped through interpretation of existing laws and creation of ad hoc legislation, resulted in a stronger protection of individuals’ rights? One cannot be so sure. In order to achieve this goal, the definition and the scope of the notion “personal data” needs to be constricted. The notion should be limited to information relating to identified individuals or that is processed in a way that allows their identification. This approach has called for a strengthening of the associated legal regime.

Despite numerous and entangled rules, the current European legal framework remains favorable to data processing and does not adequately protect freedom of self-determination. Therefore, it is of paramount importance for the existing principles to be toughened to address the risks related to the digital society. Fundamentally, the legal framework needs to evolve in a direction that guarantees a better compliance with the law by adopting a stricter and more diverse approach of monitoring and enforcing compliance. Most importantly, improvements shall be made to provide individuals better leverage to protect their data.