Université Paris II- Panthéon-Assas

École doctorale 7 – Georges Vedel – Droit public interne et comparé, science administrative et science politique

Thèse de doctorat en droit public
soutenue le 4 décembre 2019

La protection des données à caractère personnel à l'épreuve de l'automesure connectée

Thèse de Doctorat / décembre 2019

UNIVERSITÉ PARIS II
PANTHÉON-ASSAS

Maximilien LANNA

Membres du jury :

Camille BROYELLE, Professeure à l'Université Panthéon-Assas (Paris II), directrice de thèse

Lucie CLUZEL-MÉTAYER, Professeure à l'Université Paris Nanterre, directrice de thèse

M. Antony TAILLEFAIT, Professeur à l'Université d'Angers, *rapporteur*

Mme. Nathalie MARTIAL-BRAZ, Professeure à l'Université Paris Descartes, *rapporteur*

M. Gilles DUMONT, Professeur à l'Université de Nantes, *suffragant*

M. François PELLEGRINI, Professeur à l'Université de Bordeaux, *suffragant*

M. Timothée PARIS, Maître des requêtes au Conseil d'Etat, *suffragant*

AVERTISSEMENT

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

REMERCIEMENTS

Ce travail de recherche n'aurait jamais pu voir le jour sans certaines personnes, que je tiens à remercier tout particulièrement ici :

Mesdames les professeures Broyelle et Cluzel-Métayer, pour avoir accepté de diriger cette thèse et pour leur disponibilité, Madame la professeure Martial-Braz, Messieurs les professeurs Taillefait, Dumont, Pellegrini et Monsieur Paris pour avoir accepté de l'évaluer,

Monsieur le professeur Auby, ainsi que toute l'équipe de la Chaire MADP de Sciences Po, pour m'avoir accueilli et intégré à un réseau international de chercheurs,

Messieurs Perray, Belot, Desbiey, Le Grand, Rosa Salva, pour leurs conseils et éclairages,

Mes camarades doctorants, Thoma, Agathe, Anne-Laure, Antony, Morgane, Fanny, sans lesquels ce travail aurait été bien solitaire,

Tous les membres du CERSA, pour avoir fait de ce laboratoire de recherche une seconde maison,

Les personnes qui ont eu l'immense générosité de relire une partie de ce travail,

Mes amis, qui m'ont toujours soutenu,

Mes parents pour leur soutien sans faille et leur indulgence.

PRINCIPALES ABRÉVIATIONS

AFNOR	Association française de normalisation
AJCT	*Actualité juridique collectivités territoriales*
AJDA	*Actualité juridique droit administratif*
ANSSI	Agence nationale de la sécurité des systèmes d'information
API	Application programming interface
BCR	Binding corporate rules (règles d'entreprise contraignantes)
Bull.	*Bulletin des arrêts de la Cour de cassation*
Bull. civ.	*Bulletin des arrêts des chambres civiles de la Cour de cassation*
Bull. crim.	*Bulletin des arrêts de la chambre criminelle de la Cour de cassation*
BVerfG	*Bundesverfassungsgericht*
CA	Cour d'appel
CAA	Cour administrative d'appel
Cass.	Cour de cassation
CC	Conseil constitutionnel
CE	Conseil d'État
CEDH	Cour européenne des droits de l'Homme
CESDH	Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales
CEPD	Contrôleur européen de la protection des données
CGU	Conditions générales d'utilisation
Civ.	Chambre civile de la Cour de cassation
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
COM	Communication

Com.	Chambre commerciale de la Cour de cassation
Cons. Const.	Conseil constitutionnel
Crim.	Chambre criminelle de la Cour de cassation
CRPA	Codes des relations entre le public et l'administration
D.	*Recueil Dalloz*
DDHC	Déclaration des droits de l'homme et du citoyen
DGCCRF	Direction générale de la concurrence, de la consommation et de la répression des fraudes
dir.	Sous la direction de
DMP	Dossier médical personnel
éd.	Edition
EDVIGE	Exploitation documentaire et valorisation de l'information générale
Fasc.	Fascicule
FBI	Federal Bureau of Investigation
G29	Groupe de travail article 29
GAFA	Google Apple Facebook Amazon
Gaz. Pal.	*Gazette du Palais*
IBM	International Business Machines
iOS	Iphone Operating System
IOT	Internet of things
IP	Internet protocol
ISO	International organization for standardization
JCl. Adm.	*JurisClasseur Administratif*
JORF	*Journal officiel de la République française*
JOUE	*Journal officiel de l'Union Européenne*
LIL	Loi Informatique et Libertés
LPA	*Les Petites Affiches*
NIR	Numéro d'inscription des personnes au répertoire national d'identification des personnes physiques
NSA	National Security Agency
NTIC	Nouvelles technologies de l'information et de la communication

OCDE	Organisation de coopération et de développement économiques
Op. cit.	Dans l'ouvrage cité précédemment
Ord.	Ordonnance
p.	page
PbD	Privacy by design
PbU	Privacy by using
PIA	Privacy impact assessment
PUF	Presses universitaire de France
QPC	Question prioritaire de constitutionalité
QS	*Quantified-self*
Lebon T.	Tables du Recueil *Lebon*
RDP	*Revue du Droit Public*
Rec.	Recueil
Rec. Dalloz	*Recueil Dalloz*
RDSS	*Revue de droit sanitaire et social*
RGPD	Règlement général sur la protection des données
RFAP	*Revue française d'administration publique*
RFDA	*Revue française de droit administratif*
RFDC	*Revue française de droit constitutionnel*
RFID	Radio frequency identification (identification par radiofréquence)
RTD Com.	*Revue trimestrielle de droit commercial*
RTD Eur.	*Revue trimestrielle de droit européen*
SAFARI	Système informatisé pour les fichiers administratifs et le répertoire des individus
TA	Tribunal administratif
TC	Tribunal des conflits
TFUE	Traité sur le fonctionnement de L'Union européenne
TIC	Technologies de l'information et de la communication
TUE	Traité sur l'Union européenne

SOMMAIRE

Introduction

1. Le 15 janvier 2019, l'équipementier sportif américain Nike a dévoilé une paire de chaussures dédiée à la pratique du basket-ball, connectée et autolaçante[1]. Cette annonce a été suivie, quelques semaines plus tard, par la présentation d'un modèle similaire de la part de son concurrent allemand Puma[2]. Outre leurs capacités autolaçantes, ces chaussures ont pour particularité d'être reliées à une application mobile permettant d'analyser les performances sportives de leur porteur : nombre de pas parcourus, distance, intensité de la foulée ou encore nombre de calories dépensées. Inspirées de la science-fiction[3], ces chaussures sont principalement destinées aux sportifs qui souhaitent bénéficier d'informations complémentaires sur leur activité physique. Ainsi, des informations, traduites en données informatiques susceptibles d'être analysées, comparées et partagées, naissent de l'activité physique fournie par l'individu. Cette traduction nécessite, pour sa mise en œuvre, le recours à une connexion Internet. C'est en effet celle-ci qui va permettre le transfert de l'information d'un capteur à une application pour procéder à son analyse. En matière de chaussures, cette technologie favorisant le transfert en est encore à ses balbutiements. Mais celle-ci est aujourd'hui largement utilisée et de nombreux objets sont ainsi connectés à Internet afin de transmettre directement des informations.

2. La connexion à Internet d'objets du quotidien constitue en effet l'une des évolutions les plus marquantes du tournant pris par le domaine du numérique ces dernières années. Garantissant une hyperconnexion des individus, ces objets sont désormais reliés en réseau. Ils ne sont plus inertes mais dotés de capacités importantes de communication. Leur connexion à Internet leur permet non seulement de transmettre des informations en temps réel mais également de communiquer entre

[1] https://news.nike.com/news/nike-adapt-bb
[2] https://about.puma.com/en/newsroom/corporate-news/2019/2019-01-31-puma-introduces-self-lacing-training-shoe
[3] Dans le célèbre film « Retour vers le futur II » de Robert Zemeckis sorti en 1989, le héros principal, Marty McFly, fait un voyage dans le futur et découvre, dans son passage de 1985 à 2015, une paire de chaussures futuriste de la marque Nike. Ces chaussures, au laçage automatique dans le film, ont été éditées en version limitée sans cette fonctionnalité par la marque en 2011.

eux. A l'origine d'un maillage informationnel, les données émises par les objets connectés sont agrégées pour être mises en relation, et ce pour les rendre plus « riches » et plus « parlantes »[4]. Surtout, elles font l'objet d'analyses poussées par différents programmes pour que « des décisions, des choix, puissent être pris afin que des actions cognitives soient menées – ou pas »[5]. Par ailleurs, ces objets ne sont plus isolés mais s'insèrent dans un ensemble plus large et plus vaste, composé d'autres objets connectés, de réseaux, de serveurs, de logiciels de traitement et de protocoles de sécurité[6]. Cette connexion à Internet touche ainsi un ensemble élargi de dispositifs puisque n'importe quel objet est susceptible d'être connecté : voiture, transports publics, montre, brosse à dents, ampoule, réfrigérateur, pèse-personne. L'objectif de cette hyperconnexion est dès lors double, entre optimisation du fonctionnement de ces objets et retour d'informations à l'utilisateur lui permettant de guider et d'ajuster son comportement.

Ces dispositifs, pour fonctionner pleinement, se nourrissent de données. Ils intéressent le droit puisque les données traitées sont souvent des données à caractère personnel, définies comme des informations identifiantes qui se rapportent à l'individu et qui font l'objet d'une protection particulière. Les nouvelles technologies bousculent également l'utilisation qui est faite de telles données. Celles-ci deviennent en effet la source première d'alimentation de ces services et en constituent ainsi la raison d'être. Les nouvelles technologies qui sont mises en œuvre conduisent dès lors à une révélation toujours plus grande d'éléments relatifs à l'intimité et à la santé. Par ailleurs, cette modification des rapports aux données à caractère personnel est en grande partie responsable de la mutation, au cours des dernières années, du cadre juridique applicable. Celui-ci a dû faire l'objet de différentes réformes pour pouvoir prendre en compte les risques nouveaux liés à l'utilisation de données à caractère personnel, risques renouvelés par le recours croissant à des dispositifs connectés. L'émergence de ce phénomène nouveau **(I)** nécessite d'étudier le contexte juridique qui réglemente le déploiement de ces objets techniques **(II)**.

[4] Jean-Paul Crenn, « Les objets connectés décryptés pour les juristes », *Dalloz IP/IT*, 2016, p. 389.

I. L'émergence d'un nouveau phénomène

3. L'automesure connectée est une composante et une émanation à part entière du domaine des objets connectés. Elle est définie comme la « pratique consistant, pour une personne, à mesurer elle-même à l'aide d'objets connectés des variables physiologiques la concernant, relatives notamment à sa nutrition, à ses activités physiques ou à son sommeil »[7]. Son existence est antérieure à l'éclosion du marché des dispositifs connectés mais ces objets ont permis à l'automesure de s'automatiser, de gagner en efficacité et également d'être adoptée par le grand public. A l'origine réservé à un cercle d'initiés, le *quantified-self*, tel qu'il est nommé outre-Atlantique, s'est ainsi rapidement développé grâce aux évolutions technologiques. La traduction de ce terme par la Commission générale de terminologie et de néologie publiée au Journal officiel du 4 mars 2017 est révélatrice de son développement et de son acculturation. Cette adoption de l'automesure connectée **(A)** fait ainsi appel à un écosystème numérique complexe **(B)** qui repose sur l'exposition de soi **(C)**.

A. L'automesure connectée

1. La genèse de l'automesure connectée

4. La genèse d'un mouvement – L'apparition et la démocratisation du web social à la fin des années 2000 ont constitué une évolution remarquable en raison de la capacité donnée aux individus de pouvoir devenir directement créateurs de contenus en ligne. La sortie du premier téléphone iPhone par la firme américaine Apple en 2007, au moment même où les réseaux sociaux Twitter et Facebook ont connu un véritable essor, a marqué un autre tournant dans l'évolution des services numériques. Les individus ont en effet été dotés d'outils techniques mobiles, capables de tenir dans la poche et permettant d'accéder à Internet ou de partager directement des informations. L'ouverture en 2008 de l'App Store, magasin d'applications en ligne pouvant être téléchargées directement sur l'appareil, a permis de compléter cette évolution tout en posant les bases permettant le développement de l'automesure

[5] *Ibidem.*
[6] *Ibidem.*
[7] JORF, Avis divers, Commission d'enrichissement de la langue française, n° 0054, 4 mars 2017, texte 92.

connectée. En 2014, la mise sur le marché de la première montre connectée d'Apple, dite Apple Watch, a révélé au grand public l'existence de dispositifs connectés. De tels outils existaient auparavant mais étaient seulement connus et utilisés par un public averti. L'exposition médiatique propre à la firme californienne a contribué à généraliser le développement de ce type d'objets et a favorisé son adoption par un public non-averti tout en sensibilisant celui-ci à la pratique de l'automesure.

5. Considéré comme un véritable mouvement par ceux qui la pratiquent[8], l'automesure connectée s'est véritablement formalisée à partir de l'année 2007. Gary Wolf et Kevin Kelly, éditeurs du magazine américain spécialisé en nouvelles technologies, *Wired*, ont contribué à son essor en organisant les premières rencontres entre utilisateurs et fabricants d'outils de collecte de données. Ceux-ci, identifiant l'apparition d'un certain nombre de nouveaux services tels que le *life logging* ou enregistrement de différents éléments de la vie courante, la géolocalisation ou encore la biométrie et la génomique, ont cherché à mettre en évidence le lien les unissant. Les différentes observations réalisées ont montré que chacun de ces services, en ayant recours à des méthodes de calcul, permettaient aux individus de mieux se connaître[9]. Les données récoltées ne présentaient pas de spécificités particulières. En effet, l'automesure existait déjà, mais celle-ci était réalisée manuellement et sans l'aide d'outils de mesures connectés à un réseau informatique. La CNIL a proposé une définition de cette pratique, en faisant référence aux origines de ce mouvement. Elle indique ainsi que le *quantified-self* permet la « mesure de soi » et qu'il fait « référence à un mouvement né en Californie qui consiste à mieux se connaître en mesurant des données relatives à son corps et à ses activités »[10].

6. Un processus automatisé – Quatre étapes sont généralement assignées au *quantified-self* : collecte de données à partir d'une activité, analyse et comparaison des performances au regard de l'objectif poursuivi, modification du comportement au regard des résultats et recommencement du processus[11]. Ainsi, l'automesure peut être

[8] Emmanuel Gadenne, *Le guide pratique du Quantified Self, Mieux gérer sa vie, sa santé, sa productivité*, Editions fyp, 2012, 224 p.
[9] http://quantifiedself.com/2011/03/what-is-the-quantified-self/
[10] https://www.cnil.fr/fr/definition/quantified-self
[11] Mario Ballano Barcena, Candid Wueest, Hon Lau, *How safe is your quantified-self ?*, Symantec, Security Response, 2014, p. 10.

réalisée manuellement à travers différentes prises de notes, calculs, relevés horaires ou projections statistiques. Celle-ci était, à l'origine, exclusivement réalisée de cette manière. Mais le recours aux objets connectés et aux applications mobiles, permettant son informatisation et son automatisation, a favorisé son adoption par le grand public tout en renforçant la précision des informations traitées. En effet, la conversion des informations reçues en données numériques facilite leur analyse mais permet également de les croiser entre elles afin d'obtenir des résultats complémentaires autrement plus précis que si un individu y procédait manuellement et de façon isolée. L'individu peut dès lors avoir accès à des *wearables*, vêtements et accessoires d'habillements équipés de capteurs et de senseurs divers. Ceux-ci, portés en permanence par l'individu pour recueillir des informations, se caractérisent par l'automatisation du processus de création d'informations et par la permanence de cette création. Des données sont créées en continu, sans que l'individu ait à réaliser d'actions supplémentaires. Cette intelligence silencieuse engendrée par la connexion à Internet d'objets du quotidien est fondée sur la miniaturisation, l'accessibilité et le caractère sans-fil des dispositifs utilisés[12]. Ceux-ci délivrent un retour d'information précis, complet et surtout varié. La répétition de ces différentes opérations apporte par ailleurs à l'individu le matériau nécessaire pour apprécier l'évolution de ses performances, l'efficacité de l'automesure étant liée à sa répétition dans le temps.

2. L'essor de l'automesure connectée

7. La pratique de l'automesure est aujourd'hui favorisée par un certain nombre de facteurs convergents. Le véritable dogme de la mesure qui est à l'œuvre est en effet rendu possible par une explosion du nombre de données analysées et qui contribue ainsi à l'essor de nouveaux acteurs.

8. Le dogme de la mesure – L'objectif assigné à l'automesure connectée est relativement simple. Il permet à l'individu d'obtenir des informations sur différents éléments de sa vie quotidienne : nombre de calories ingérées ou dépensées, qualité du sommeil, nombre de pas parcourus au cours d'une même journée, temps de déplacement, géolocalisation ou encore rythme cardiaque. La liste des éléments

[12] Daniel Kellmereit, Daniel Obodovski, *The Silent Intelligence, the Internet of Things*, DND Ventures, 2013, p. 14.

pouvant entrer dans le domaine du *quantified-self* n'est pas exhaustive et varie au gré des différents besoins des individus. Le seul dénominateur commun étant le rapport au corps humain de la personne afin que celle-ci soit en mesure de mieux se connaître et d'adapter son comportement en fonction des résultats qui lui sont transmis. Les athlètes et sportifs occasionnels étaient à l'origine les principaux concernés par ces retours d'informations mais ce procédé s'est progressivement démocratisé avec l'avènement d'un dogme de l'évaluation qui est désormais appliqué au corps humain. En relevant des éléments tels que la perte ou le gain de poids, l'amélioration des cycles de sommeil ou les performances physiques et sportives, le *quantified-self* repose sur l'évaluation des progrès réalisés dans le temps par l'individu, sur sa notation ou encore son classement par rapport à un groupe donné d'utilisateurs[13]. Ce phénomène de notation, mis en œuvre et observé dans le cadre de l'automesure, s'insère actuellement dans un mouvement plus global d'évaluation : hôtels, restaurants, chambres d'hôtes[14], magasins, hôpitaux[15] ou encore services publics[16] et politiques publiques y sont tous soumis et c'est désormais au corps humain et à l'individu que s'appliquent ces mécanismes.

9. L'élaboration d'un soi commensurable car chiffré renvoie bien à « l'obsession contemporaine pour une objectivité qui passe par la mise en nombres »[17]. Dès 2014, le laboratoire d'innovation numérique de la CNIL (LINC) consacrait un cahier entier à l'automesure connectée. Le choix de son titre, *Le corps, nouvel objet connecté*, corrobore cette notion d'évaluation appliquée au corps humain, propre à la quantification de soi. Reprenant et citant les travaux d'Alain Desrosières relatifs à la gouvernance par les nombres, le cahier de la CNIL rappelle que quantifier consiste à « exprimer et faire exister sous une forme numérique ce qui,

[13] L'application de course à pieds et d'entraînement sportif *Pumatrac*, disponible sur smartphones et tablettes, propose un classement de ses utilisateurs en fonction des performances réalisés.
[14] Le développement de sites Internet dédiés à la notation de services tel que *Trip Advisor* pour les hôtels et restaurants a contribué à la démocratisation de ce genre de pratiques.
[15] L'hebdomadaire français Le Point propose chaque année un palmarès des hôpitaux en fonction des spécialités médicales.
[16] Voir notamment : Delphine Dero-Bugny, Aurore Laget-Annamayer (dir.), *L'évaluation en droit public*, Actes du colloque du 16 mai 2014, Presses Universitaires de Clermont-Ferrand, 2014, 240 p. ; Charlotte Agulhon, *Le contrôle juridictionnel des évaluations en droit public*, Thèse pour le doctorat en droit présentée et soutenue publiquement le 20 juin 2019, Université Paris-I Panthéon-Sorbonne ; Stéphane Le Bouler, « Évaluer les services publics : l'exemple de la santé », *Regards croisés sur l'économie*, vol. 2, no. 2, 2007, p. 206 à 215.
[17] CNIL, *Le corps, nouvel objet connecté, Du quantified-self à la M-Santé : les nouveaux territoires de la mise en données du monde*, Cahiers IP, Innovation & Prospective, n°2, 2014, p. 4.

auparavant, était exprimé par des mots et non par des nombres »[18]. Tel est l'objet du *quantified-self* qui, par la mesure de variables relatives au mode de vie, a pour objectif de mettre en nombre l'individu afin de procéder à son évaluation. Surtout, à l'image des procédés de notation de services précédemment cités, ces pratiques d'automesure « contribuent à redéfinir continuellement des objectifs de performance et de jouissance de manière à inscrire les individus dans des processus de perfectionnement dont l'objectif recule au fur et à mesure qu'ils progressent »[19]. Les données relevées permettent donc à l'individu d'influencer son propre comportement et d'agir en fonction d'objectifs mesurables. Cette gouvernance par les nombres, telle qu'elle est décrite par le professeur Alain Supiot, vise la programmation de l'agir humain et affecte donc nécessairement le statut et l'identité des individus[20]. Par ailleurs, l'idée de perfectionnement associée à l'automesure est renforcée par l'idée de communauté qui entoure cette pratique, les individus pouvant partager leurs résultats afin de les comparer. Loin de se cantonner au domaine sportif, cette recherche de la performance touche désormais tous les aspects de la vie quotidienne.

10. Plusieurs éléments ont contribué à la démocratisation de tels processus. L'apparition des smartphones semble être l'élément déclencheur du développement d'autres outils présentant une technologie similaire ou s'appuyant sur la technologie embarquée desdits *smartphones*. Le développement d'applications mobiles téléchargeables via différentes plateformes en ligne a contribué à la spécialisation des différentes composantes de l'automesure connectée. A chaque constante du corps humain pouvant faire l'objet d'une mesure correspond une application mobile aux capacités de calcul renforcées. La transformation de l'automesure repose donc sur l'utilisation d'objets et dispositifs connectés : ce sont eux qui permettent le passage de l'automesure à l'automesure connectée. Les différents dispositifs ainsi que leurs caractéristiques seront présentés ultérieurement, mais un dénominateur commun doit d'ores et déjà être identifié : ces dispositifs permettent la traduction d'une information en une donnée informatique, susceptible d'être analysée et comparée. Cette mise en données des informations permet non seulement de faciliter les

[18] Alain Desrosières, *Pour une sociologie historique de la quantification. L'argument statistique I*, Presses de l'École des mines, 2008, pp. 10-11.
[19] CNIL, *op. cit.*, p. 5.
[20] Alain Supiot, *La Gouvernance par les nombres, Cours au collège de France 2012-2014*, Fayard, 2015, p. 216.

capacités d'analyse mais elle facilite également le partage de ses propres résultats avec d'autres utilisateurs. Cela permet à l'individu de comparer son activité et également de bénéficier de conseils ou de soutien. La notion de communauté qui existait déjà avec l'automesure est renforcée par sa connexion à Internet et par son automatisation, les capacités de partage et de comparaison des résultats étant renforcées et surtout facilitées.

11. La particularité des objets connectés et ce qui en constitue la spécificité, est de reposer sur une collecte exponentielle de données. On estime que 2, 5 trillions d'octets de données sont produites chaque jour et que 90% d'entre elles ont été créées au cours des dernières années[21]. Cette collecte croissante de données constitue la valeur ajoutée de ces dispositifs : leur objectif est en effet de pouvoir apporter le plus d'informations possible aux utilisateurs afin d'aider à la prise de décision ou à la modification de certains comportements, à chacun des niveaux déjà mentionnés. Un individu pourra ajuster son rythme de sommeil en fonction des informations qui seront délivrées par son *tracker* d'activité, bracelet connecté permettant de relever des données en continu. Les données, par leur nombre, leur diversité et leur qualité, s'insèrent à l'heure actuelle dans un ensemble plus vaste, dénommé *big data* ou grand ensemble de données. Celui-ci fait référence à « la collecte et à l'agrégation de grandes masses de données provenant de différentes sources, dans le but d'extraire de nouvelles informations grâce à des analyses statistiques, descriptives ou prévisionnelles »[22]. Le *big data* désigne ainsi la pratique visant à collecter un ensemble indifférencié de données. Celles-ci peuvent concerner directement ou non les individus et le fait de procéder à leur analyse est appelé le *data mining*[23].

12. La puissance des algorithmes – Le risque de ne pas pouvoir traiter avec efficacité l'ensemble des données créées a pu être soulevé mais celui-ci s'est dissipé au regard de l'évolution de la capacité de calcul des ordinateurs. Le *big data*, envisagé comme la compréhension et l'interprétation d'ensembles non structurés

[21] Simon Chignard, Louis-David Benyayer, *Datanomics*, Editons Fyp, 2015, p. 17.
[22] Danièle Bourcier, Primavera De Filippi, *Open Data & Big Data, Nouveaux défis pour la vie privée*, Mare & Martin, Droit & Sciences Politiques, 2016, p. 33.
[23] Bruce Schneier, *Data and Goliath*, W.W. Norton & Company, 2016, p. 29.

d'informations dont le sens n'était jusqu'à présent que limitativement perçu[24] a permis de conférer une réelle utilité au *quantified-self*. Les applications mobiles jouent dès lors un rôle particulier puisque ce sont elles qui permettent l'analyse des données collectées et qui permettent dès lors une réelle exploitation des informations relatives aux individus. Ainsi, la numérisation de l'automesure et la croissance exponentielle du nombre d'informations traitées se sont accompagnées d'une modification profonde des modes d'analyse de telles informations, notamment par le recours à des algorithmes. Présents dans nos objets du quotidien, comme la machine à café, le distributeur automatique, la voiture automatique ou encore l'ordinateur, ils sont susceptibles de remplir trois fonctions : agir sur la décision humaine en l'influençant, se substituer à la décision humaine ou enfin, prédire la décision humaine[25]. Ceux-ci sont « nés du besoin de trouver des solutions rapides et efficaces par la transformation de données à l'aide de directives précises appliquées par étapes successives »[26] et rendent possible le traitement efficace du flot important de données collectées. Ce développement de procédés de calcul permettant aux ordinateurs de trier, de traiter et d'agréger les informations n'est pas propre au *quantified-self* mais il soulève néanmoins la question du caractère ubiquitaire des dispositifs employés. En effet, alors que « les objets qui nous environnent cherchent à désenclaver les mesures de leur enclos numérique pour se glisser dans les activités quotidiennes » et qu'ils ouvrent d'immenses possibilités, ceux-ci « posent en revanche de redoutables questions quant à la gouvernance de ces nouvelles données »[27].

13. La gouvernementalité algorithmique. Le développement du *quantified-self* s'inscrit dans la lignée d'un concept identifié sous l'appellation de « gouvernementalité algorithmique »[28]. En effet, « les nouvelles opportunités d'agrégation, d'analyse et de corrélations statistiques au sein de quantités massives de données (les *big data*), nous éloignant des perspectives statistiques traditionnelles de l'homme moyen, semblent permettre de « saisir » la « réalité sociale comme telle, de

[24] Viktor Mayer-Schönberger, Kenneth Cukier, *Big Data, A Revolution That Will Transform How We Live, Work and Think*, John Murray, 2013, p. 19.
[25] Jean-Baptiste Duclercq, « Le droit public à l'ère des algorithmes », *Revue du Droit Public*, n° 5, 2017, p. 1402.
[26] *Ibid.*
[27] Dominique Cardon, *A quoi rêvent les algorithmes, nos vies à l'heure des big data*, La République des Idées, Seuil, 2015, p. 11.
[28] Antoinette Rouvroy, Thomas Berns, « Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? », *Réseaux*, vol. 177, n°1, 2013, p. 163 à 196.

façon directe et immanente, dans une perspective émancipée de tout rapport « à la moyenne » ou à la « normale », ou, pour le dire autrement, affranchie de la « norme » »[29]. Complémentaire, bien qu'éloigné des usages traditionnels d'outils statistiques, le recours à l'automesure connectée dans le cadre du *big data* permet d'agir sur le comportement des individus. Les objets utilisés dans le cadre de l'automesure participent à la production d'un savoir automatisé à partir d'un nombre important d'informations, ce savoir étant par la suite mis à disposition des individus. Or, la mise en nombre grâce au *quantified-self* a une double influence sur le comportement de la personne : celle-ci l'adapte directement en fonction des informations qu'elle reçoit tout en étant également soumise à l'appréciation des tiers.

14. L'explosion des données – L'analyse et la corrélation de données agrégées et ne présentant pas d'intérêt intrinsèque permet d'apporter une plus-value aux informations initialement collectées. Le *quantified-self* s'insère directement dans la lignée de ce type d'analyse. La véritable valeur ajoutée du service proposé repose sur l'accumulation constante de données de nature différente. Surtout, la routinisation du processus de collecte permet *in fine* de conférer toute son utilité aux dispositifs connectés utilisés. L'exemple d'un athlète souhaitant mesurer son activité physique est à ce titre particulièrement révélateur. Les mesures obtenues lors d'une unique course à pieds ne pourront pas véritablement servir d'indicateur à l'individu. En revanche, la répétition quotidienne ou hebdomadaire de ce procédé implique réellement l'exploitation des informations traitées puisqu'elle permet de procéder à des comparaisons et à des corrélations entre différents jeux de données, illustrant par ailleurs le nouveau rapport au corps qu'implique le *quantified-self*. Ces différentes opérations permettront à l'utilisateur de bénéficier d'une analyse précise de son activité. Dès lors, les individus pratiquant l'automesure connectée sont invités à fournir un nombre important de données permettant généralement de les identifier.

Les données tendent « à devenir le carburant essentiel de toute action sociale, qu'elle soit économique ou non »[30]. Cette affirmation est corroborée par la pratique de l'automesure connectée car ce sont les données collectées, relatives aux individus,

[29] *Ibid.*
[30] Jean-Bernard Auby, « Le droit administratif face aux défis du numérique », *AJDA*, 2018, p. 835.

qui vont conférer une vraie valeur ajoutée aux services utilisés. Cette valeur qui est associée à la donnée est double. D'une part, elle permet de renforcer le caractère attractif du service proposé en alimentant celui-ci d'informations et d'autre part, elles représentent un atout pour les sociétés à l'origine des services proposés. En effet, à l'image des différentes révolutions industrielles qui ont toutes eu pour point de départ l'exploitation d'un type d'énergie nouveau, ce sont aujourd'hui les données créées directement par les individus qui constituent un nouveau gisement de valeur, susceptible également de relancer l'innovation, la productivité et la croissance. La notation appliquée aux habitudes de vie des personnes utilisant des dispositifs connectés est créatrice de valeur pour les entreprises proposant leurs services. En effet, les informations traitées servent de base au modèle économique déployé qui repose en grande partie sur le ciblage publicitaire et sur la connaissance des utilisateurs desdits services. Le marketing et la publicité ciblée axés sur la donnée génèrent ainsi plus de 150 milliards de dollars par an[31]. La valorisation économique progressive de la donnée a été rendue possible par le développement d'un écosystème numérique toujours plus complexe qui repose en partie sur le développement de plateformes numériques.

15. Le développement des plateformes – Le processus de numérisation de nos sociétés est aujourd'hui couplé à un phénomène dit d'ubérisation. Celui-ci vise à une redéfinition du rôle des intermédiaires ou à leur suppression dans la mise en œuvre d'une économie de plateforme. Entendues comme des « interfaces d'intermédiation ouvertes, sur lesquelles les fournisseurs et les clients se retrouvent virtuellement »[32], les plateformes mettent directement en relation des utilisateurs et des fournisseurs. Celles-ci contribuent donc au phénomène de désintermédiation, défini par le Conseil d'Etat comme un « phénomène économique favorisé par l'émergence d'Internet et de l'économie des plateformes et se traduisant par la réduction, voire la suppression des intermédiaires dans un circuit de distribution »[33]. Les opérateurs du numériques impliqués dans le domaine de l'automesure connectée

[31] Frank Pasquale, *Black Box Society : les algorithmes secrets qui contrôlent l'économie et l'information*, éditions fyp, 2015, p. 36.
[32] Conseil d'Etat, *Puissance publique et plateformes numériques : accompagner l'« ubérisation »*, Etude annuelle, La documentation française, 2017, p. 26.
[33] *Ibid.*

s'apparentent, pour certains, à des plateformes qui « mettent en relation plusieurs faces (ou groupes) d'utilisateurs qui ne peuvent à eux seuls et mutuellement capturer la valeur de leurs interactions »[34]. Malgré un manque de définition unifiée, les écosystèmes d'applications mobiles permettant de collecter et de traiter les données ou les réseaux sociaux rendant possible leur partage ont été identifiés par la Commission européenne comme faisant partie des grandes catégories de plateforme[35].

Le rôle des plateformes en matière d'automesure connectée mérite d'être souligné. D'abord, l'utilisation d'objets connectés pour procéder aux mesures permet une individualisation toujours plus poussée des services proposées. Plus les informations transmises par les individus sont nombreuses et détaillées, mieux le service pourra s'adapter aux besoins et attentes de l'individu. L'application de *running* de la firme Nike constitue un exemple frappant : l'individu, après avoir renseigné sa taille et son poids, peut bénéficier de conseils d'entraînement qui sont fondés sur l'analyse de ses précédents efforts. L'application s'adapte à l'individu en fonction des données que celui-ci fournit lors de séances sportives. Ensuite, cette logique de plateforme conduit à la centralisation, entre les mains de mêmes opérateurs, d'un nombre important de données concernant l'individu et qui sont collectés à travers les différents services proposés par une même plateforme. Un changement de rapport aux outils informatiques, favorisé par ce développement de plateformes, est ressenti jusque dans le domaine de la santé, comme le démontre d'ailleurs « la « course » entre Google et Apple, par exemple, pour le développement de la collecte, de l'analyse et du traitement des données de santé »[36].

3. Le lien entre bien-être et santé connectée

16. L'automesure connectée a pour particularité de brouiller les frontières entre le domaine du bien-être et celui de la santé. Cette confusion est renforcée par la définition de la santé adoptée dès 1946 par l'Organisation mondiale de la Santé (OMS). Pour celle-ci, la santé est « un état de complet bien-être physique, mental et

[34] Winston Maxwell, Thierry Pénard. « Quelle régulation pour les plateformes numériques en Europe ? », *Annales des Mines - Réalités industrielles*, vol. août 2016, n° 3, 2016, p. 42 à 46.
[35] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, *Les plateformes en ligne et le marché unique numérique, Perspectives et défis pour l'Europe*, COM (2016) 172.
[36] Conseil d'Etat, *op. cit.*, p. 62.

social, et ne consiste pas seulement en une absence de maladie ou d'infirmité ». Le *quantified-self* entend justement procéder à une mesure d'éléments relatifs au bien-être, qu'il s'agisse d'indicateurs propres à l'activité sportive ou par exemple au sommeil ou à la nutrition, mais aussi à des éléments relatifs à la santé, tels que le taux de glycémie. Le développement de l'informatique a en effet également profité au domaine de la santé en permettant son informatisation. Deux phénomènes distincts ont progressivement pu voir le jour : la cybersanté et la santé mobile.

17. La cybersanté ou santé connectée, qui consiste à utiliser les technologies de l'information et de la communication à l'appui de l'action de santé[37], s'est aujourd'hui généralisée. En ayant recours à ces technologies, entendues comme « une combinaison de produits et de services qui capturent, enregistrent et affichent des données et des informations, par voie électronique »[38], de nombreux services nouveaux ont pu être mis en œuvre. Qu'il s'agisse de la mise en œuvre de dossiers électroniques de patients au sein des hôpitaux ou du remboursement électronique de soins, les nouvelles technologies ont permis le développement de ces services innovants et connectés.

18. Ce développement de la cybersanté a été suivi par l'apparition de la santé mobile, également appelée *mHealth*. L'OMS en donne une définition dès 2011 et considère qu'il s'agit de « pratiques médicales et de santé publique supportées par des appareils mobiles, tels que les téléphones mobiles, les dispositifs des patients, les PDA et autres appareils sans fil »[39]. La santé mobile permet donc par exemple à l'individu de consulter son dossier médical à distance grâce à son *smartphone* ou encore de relever certaines mesures grâce à un dispositif connecté, tel qu'un capteur de glycémie. Intégrée à la cybersanté, elle en constitue une subdivision particulière en raison du critère relatif à la mobilité qui lui est associé. Le développement progressif des *smartphones* et l'utilisation d'objets connectés a donc permis à la santé connectée de devenir mobile, de sortir du cadre hospitalier et ainsi d'être adoptée par un plus grand nombre d'individus et de praticiens. Le rattachement du *quantified-self* à la

[37] Organisation Mondiale de la Santé, *Cinquante-huitième Assemblée Mondiale de la Santé*, Résolutions et décisions, annexe, Genève, 2005, p. 114.
[38] OECD, *Measuring the Information Economy*, Annex 1., The OECD Definition of the ICT Sector, 2002, p. 81.
[39] World Health Organization, *mHealth, New horizons for health through mobile technologies*, 2011, p. 6.

santé connectée ou à la santé mobile peut donc être direct mais également indirect, en raison des informations collectées.

La particularité du *quantified-self* est de pouvoir, dans certains cas, être inclus au domaine de la santé mobile. Cette ambiguïté est confortée par l'utilisation d'objets connectés, outils permettant de mesurer des éléments relatifs à l'activité physique et donc au corps humain. Dès lors, on constate que les frontières sont « de plus en plus brouillées dans le monde de la santé connectée et il devient difficile, voire aléatoire, de faire une distinction absolue entre les dispositifs, applications et objets connectés utilisés dans le domaine du bien-être, dans celui de la santé et dans celui de l'exercice de la médecine »[40]. Le *quantified-self* redessine ainsi la frontière entre le domaine du bien-être et celui de la santé : afin de relever des informations qui en sont théoriquement éloignées, telles que le nombre de pas parcourus en une journée ou l'évolution du poids, le *quantified-self* génère des informations qui, lorsqu'elles sont interconnectées, permettent de tirer des conclusions relatives à l'état de santé d'une personne. Les dispositifs d'automesure connectée peuvent donc, selon leur vocation première, être utilisés dans un cadre ludique et récréatif. Mais ces dispositifs peuvent également compléter un parcours de soin traditionnel en collectant des informations relatives à la santé de l'individu. Cette confusion des domaines du bien-être et de celui de la santé a, comme nous le verrons, des incidences sur la qualification juridique qui est apportée aux données traitées et donc sur le régime juridique qui leur est applicable.

Un écosystème numérique se met en place, composé d'objets et instruments en communication et interaction permanente et celui-ci contribue à entretenir le flou quant aux différentes qualifications juridiques à retenir.

B. Un écosystème numérique complexe

19. Web 3.0 et Internet des objets – L'Internet des objets s'insère dans le Web 3.0 ou troisième évolution de l'Internet. Il peut être défini comme « une infrastructure mondiale pour la société de l'information, qui permet de disposer de

[40] Conseil National de l'Ordre des médecins, *Santé Connectée, De la E-Santé à la Santé Connectée, Le Livre Blanc du Conseil National de l'Ordre des médecins*, janvier 2015, p. 9.

services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution »[41]. Contrairement au Web 2.0 ou web social, ce ne sont plus les individus qui interagissent entre eux, mais les objets directement entre eux et par extension, avec les individus. Cette capacité d'interaction est révélatrice d'une des caractéristiques essentielles de l'Internet des objets et qui a trait à l'interconnectivité ou interconnexion des objets utilisés. Celle-ci permet de croiser les informations issues de sources diverses pour fournir à l'individu des résultats toujours plus fiables et précis. Le terme d'Internet des objets aurait été employé pour la première fois en 1999 par un chercheur américain à propos des puces RFID (*Radio Frequency Identification*) permettant le déploiement d'objets connectés capables de dialoguer entre eux[42]. Ces puces permettent l'identification unique de ces objets et donc leur communication et leur interaction avec d'autres dispositifs. La technologie RFID n'est pas la seule utilisée mais elle sert à définir les objets connectés comme « un réseau de réseaux qui permet, via des systèmes d'identification électronique normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant »[43].

20. Lois de Moore – L'évolution technologique des objets connectés s'inscrit dans le schéma des « lois de Moore ». Exprimées entre 1965 et 1975 par Gordon E. Moore, l'un des fondateurs de la firme Intel[44], elles indiquent, en substance, que le nombre de transistors par circuit de même taille double, à prix constants, tous les ans ou tous les dix-huit mois, exprimant concrètement la croissance exponentielle de la puissance de calcul des ordinateurs. Ces lois se vérifient à travers l'évolution technique des objets connectés, qu'il s'agisse de la première lampe connectée au réseau Wi-Fi apparue en 2003, des smartphones de dernière génération embarquant

[41] Union Internationale des télécommunications, *Présentation générale de l'Internet des objets, Secteur de la normalisation des télécommunications de l'UIT*, Y. 2060, juin 2012, p. 1.
[42] Kevin Ashton, « That 'Internet of Things' Thing », *RFID Journal*, June 22, 2009.
[43] Pierre-Jean Benghozi, Sylvain Bureau, Françoise Massit-Folléa, *L'internet des objets, quels enjeux pour l'Europe ?*, Editions de la Maison des sciences de l'homme, 2009, p. 16.
[44] Gordon E. Moore, « Cramming more components onto integrated circuits », *Electronics*, Volume 38, Number 8, April 19, 1965.

différents capteurs ou encore des montres connectées. Les différents objets en question ont vu leurs capacités techniques croître et leurs prix de vente baisser. Par ailleurs, la miniaturisation des capteurs embarqués a permis une diversification des fonctionnalités des objets proposés dans le commerce, afin de toucher progressivement tous les domaines de la vie courante. Surtout, leurs modes de fonctionnement se sont diversifiés : certains objets nécessitent de fonctionner en lien avec des applications mobiles permettant d'en extraire les résultats afin de les analyser et d'autres se sont autonomisés et délivrent un retour direct d'informations à l'utilisateur, sans média supplémentaire. Toujours plus performants, les objets connectés ont désormais vocation à être utilisés dans des contextes divers.

21. Domaines d'application variés – Plusieurs catégories d'objets connectés peuvent être identifiés en fonction de leurs usages. En effet, les dispositifs utilisés reposent tous sur la même technologie mais ils ont vocation à s'insérer dans différents environnements et à différentes échelles. L'écosystème des objets connectés s'est ainsi d'abord développé à partir du corps humain, avec le développement de capteurs personnels et *trackers* d'activité permettant aux individus de mesurer leurs efforts physiques ou des constantes relatives au bien-être. Le développement des premiers *smartphones* a rendu possible l'implémentation de cette première couche d'objets connectés et ceux-ci se sont presque conjointement déployés au sein des habitations. Dénommée domotique, celle-ci s'entend de l'ensemble des techniques de gestion automatisée qui sont appliquées à l'habitation. Les objets connectés ont dès lors permis de commander à distance différents éléments propres aux habitations, qu'il s'agisse de l'éclairage ou de la surveillance à distance. Enfin, la dernière plateforme dans laquelle se sont développés les objets connectés est celle de la ville, dans le cadre des *smart cities* notamment[45]. Les objets connectés contribuent ainsi, à l'échelon le plus large, à l'automatisation de certains processus. Collecte de déchets, gestion du trafic routier ou des dépenses énergétiques des habitations sont autant d'éléments susceptibles d'être optimisés par le recours à des objets connectés chargés de collecter des données. Différentes modalités d'utilisation

[45] Jean-Bernard Auby, « Les *smart cities* : un cadre nouveau pour les politiques sanitaires et les systèmes de santé ? », *in* Antony Taillefait, Maximilien Lanna (dir.), *Smart Cities & Santé*, Institut Universitaire Varenne, « Collection Colloque & Essais », 2019, p. 11.

sont donc possibles : un individu pourra ajuster son rythme de sommeil en fonction des informations délivrées par son tracker d'activité ou encore modifier sa consommation d'électricité en fonction du retour effectué par son compteur communicant. Les municipalités, quant à elles, pourront par exemple déterminer avec plus de précision et d'efficacité les modalités de ramassage des ordures.

22. La multiplicité des acteurs – La mise en œuvre et le développement du *quantified-self* reposent sur une diversité d'acteurs ainsi que sur une multiplication de dispositifs susceptibles d'interactions. Désormais démocratisé, ce modèle s'appuie en effet sur la mise en réseau de différents objets et instruments qui contribuent à la transmission, par les individus, d'un nombre important d'informations en vue d'obtenir des analyses et avis sur leur activité physique et leur mode de vie. Ce procédé est fondé sur une interconnexion entre un dispositif connecté ou un smartphone doté de capteurs et une application, gratuite ou non et il favorise la circulation d'un nombre toujours plus grand d'informations. Le développement du *cloud computing*, informatique en nuage, permet quant à lui le stockage externalisé d'informations et il contribue également grandement au développement de l'automesure connectée. Les données créées ne sont donc plus nécessairement directement stockées sur le dispositif, mais peuvent être conservées à distance. Une relation tripartie est donc instaurée, du dispositif connecté au *cloud* en passant par l'application mobile. Elle implique la collaboration de différentes entités, chacune spécialisées dans l'un des domaines. La mise en œuvre de l'automesure connectée a donc pour particularité de reposer sur la collaboration de différents opérateurs, qui auront tous accès aux informations transmises par l'individu.

La nature de ces opérateurs est variée : généralement privés, ceux-ci peuvent également être publics lorsque les opérations d'automesure sont réalisées à des fins sanitaires et dans un cadre hospitalier. En cela, un véritable écosystème du *quantified-self* a tendance à se développer. De nombreux opérateurs ont ainsi vocation à intervenir dans la mise en œuvre de l'automesure connectée : fabrication de l'objet utilisé, système d'exploitation de l'objet, collecte de l'information, analyse ou encore stockage de celle-ci. La mise en relation de ces différents acteurs, souvent par le recours à la sous-traitance, est rendue nécessaire par la diversité des opérations

réalisées dans le cadre de l'automesure et qui convergent toutes vers de nouvelles modalités d'exposition de soi par l'individu.

C. L'exposition de soi

23. Le paradoxe de la vie privée – L'apparition du web-social et des réseaux sociaux a entraîné une première phase d'exposition de soi pour les individus. Ceux-ci ont été encouragés, par le biais d'outils ludiques, à dévoiler de plus en plus d'éléments relatifs à leur vie privée. Ce phénomène est révélateur du paradoxe de la vie privée qui touche les internautes : sensibles aux problématiques relatives à la protection de leurs données, ils ont tendance à en révéler toujours plus en échange d'un certain nombre de services[46]. Une opposition existe donc entre d'une part, la méfiance ressentie à l'égard d'une collecte généralisée de données personnelles et d'autre part, la tendance à se dévoiler grâce aux services qui sont proposés. Apparu en même temps que les réseaux sociaux, ce paradoxe est également révélateur des différents degrés de confiance que les individus accordent aux opérateurs privés et aux opérateurs publics. Un exemple, particulièrement marquant sur ce point, concerne le projet de fichier de police informatisé « Edvige » créée en juin 2008. Visant à centraliser un nombre important d'informations, ce fichier a fait l'objet de nombreuses critiques de la part de l'opinion publique et de nombreux recours ont été formés devant le Conseil d'Etat afin d'en contester la légalité. Etabli à l'occasion de la création de la nouvelle Direction centrale du renseignement intérieur, ce fichier, qui comprenait notamment les « signes physiques particuliers et objectifs, photographies et comportement » ou encore les « données relatives à l'environnement de la personne »[47], a finalement été abandonné en novembre 2008. Au même moment pourtant, le réseau social Facebook connaissait une ascension fulgurante. Cent millions d'utilisateurs y étaient alors inscrits dans le monde, au troisième trimestre de l'année 2008[48]. Les modalités de recueil des informations sur ces deux différents supports n'étaient certes pas les mêmes : recours au consentement, volonté de l'utilisateur et choix des informations partagées les distinguaient notamment.

[46] Voir notamment sur ce point : Susan B. Barnes, *A Privacy Paradox : Social Networking in the United States*, First Monday, vol. 11, April 2006.
[47] Décret n° 2008-632 du 27 juin 2008 portant création d'un traitement automatisé de données à caractère personnel dénommé « EDVIGE ».
[48] https://fr.statista.com/statistiques/565258/facebook-nombre-d-utilisateurs-actifs-mensuels-dans-le-monde/#0

Pourtant, la démocratisation de ce type de réseaux a contribué à une modification profonde du rapport à la vie privée et les réseaux sociaux ont contribué à l'émergence de modèles économiques nouveaux : « l'implication de l'utilisateur y est toujours centrale et la monétisation des données personnelles présente partout »[49]. Ces plateformes numériques sont apparues comme des dépositaires particuliers de données personnelles et en sont devenues des gardiens dont le modèle « repose autant sur elles que sur la confiance des utilisateurs »[50]. Les services proposés se sont nourris des informations relatives aux individus, ces derniers étant constamment appelés à révéler des données les concernant afin de bénéficier de prestations en ligne.

L'automesure connectée repose aujourd'hui sur un mécanisme similaire. L'aspect ludique, convivial et bénéfique pour le bien-être associé au *quantified-self* conduit les utilisateurs à confier des informations particulièrement intimes à des tiers qui vont ensuite les monétiser. Le modèle économique reposant sur la fourniture de données personnelles en échange de services, renouvelé par le recours aux objets connectés dans le cadre de l'automesure, s'inscrit donc dans le prolongement du *privacy paradox* propre à l'économie numérique actuelle. Les entreprises développant des applications les proposent au téléchargement gratuitement, en échange de la fourniture, par les individus, de données les concernant. Ainsi, les entreprises sont rémunérées par l'exploitation de ces informations à des fins publicitaires. La précision ainsi que la diversité des données collectées permettent alors le déploiement d'une publicité particulièrement ciblée à destination des utilisateurs. L'achat de dispositifs connectés (pèse-personne ou *tracker* d'activité) permet en théorie d'échapper à cette éventualité. Mais les capteurs dont sont désormais équipés les smartphones, exploités par des applications mobiles gratuites, ont permis la généralisation de ce modèle économique. De plus, les dispositifs connectés spécifiquement dédiés au *quantified-self* peuvent être connectés aux applications librement téléchargeables. Par ailleurs, un modèle intermédiaire de type *freemium* est dans certains cas mis en place. Les fonctionnalités de base d'une application sont gratuites mais l'utilisateur doit payer pour pouvoir profiter de fonctionnalités plus

[49] CNIL, *Vie privée à l'horizon 2020, Paroles d'experts*, Cahier IP, Innovation & Prospective, n° 1, 2012, p. 15.

évoluées. Dès lors et dans ce cas de figure, les entreprises développant des applications peuvent également avoir accès aux informations des individus.

Cette transmission d'informations est doublement justifiée. D'une part, elle permet au service d'automesure d'être pleinement délivré et d'autre part, elle est rendue nécessaire par le modèle économique qui a été déployé. Les applications développées sont majoritairement gratuites et les informations transmises par les individus servent de contrepartie aux fournisseurs de service afin que ceux-ci puissent les exploiter.

24. Le profilage – Cette interdépendance, caractérisée par la transmission de données à caractère personnel en échange d'un service théoriquement gratuit, a une influence sur le rapport à la vie privée qu'entretiennent les individus. L'utilisation de différents services connectés et interconnectés ainsi que le recours à des dispositifs reliés à un réseau Internet et transmettant des informations en continu sont à l'origine d'opérations de profilage des individus. Entendu comme « toute forme de traitement automatisé de données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique »[51], le profil est déterminé par les données que les individus transmettent consciemment aux firmes du numérique en échange de services innovants. Données de géolocalisation relatives aux déplacements, aux lieux de travail, données relatives aux habitudes alimentaires, à l'activité sportive ou encore aux rythmes de sommeil sont autant d'éléments que les prestataires de service de *quantified-self* ont à leur disposition. Ils sont dès lors en mesure de dresser des profils détaillés des individus, profils renforcés par les interconnexions et différents croisements qui sont susceptibles d'être réalisés entre les jeux de données provenant de sources différentes. Par ailleurs, le traitement algorithmique de plus en plus sophistiqué de ces informations est à même de renforcer la précision des profils établis et est donc susceptible de constituer une intrusion dans la sphère privée, symptomatique d'un « empiètement de l'Etat et des entreprises sur nos droits et

[50] *Ibid.*
[51] Article 4, 4°, Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

libertés fondamentales, et notamment le droit à la vie privée »[52]. Cette sphère devient cependant monnayable, avec l'avènement du web social, « construit autour des différentes facettes de l'identité numérique »[53].

25. L'identité numérique – L'identité numérique d'un individu est potentiellement différente de son identité juridique. Différents pseudonymes ou avatars peuvent être employés pour l'utilisation de services en ligne, contribuant ainsi à la création d'une identité distincte de l'identité véritable de la personne[54]. L'identité se présente traditionnellement sous une triple dimension : personnelle[55], interpersonnelle[56] et sociale[57]. L'identité est donc d'abord subjective mais elle est également le produit d'interactions sociales, co-construite par la relation à autrui.

Le numérique procède à une redistribution de ces éléments et influence directement cette définition classique. Outre l'identité civile et le recours à des pseudonymes, perçus comme l'identité en tant qu'écran « de projection et de protection », le numérique permet le développement d'un « continuum qui accepte toutes les nuances et les variantes de l'inscription identitaire »[58]. Les échanges réalisés grâce aux outils numériques sont dès lors dans la continuité de ceux réalisés dans le monde réel, mais ils peuvent également en être totalement dégagés. A ce titre et à l'image d'un pseudonyme qui peut également « servir à marquer un autre aspect de l'identité, plus subjectif, souvent affectif »[59], l'identité numérique apparaît comme étant une identité augmentée, produit des interactions dans le monde réel et sur Internet.

L'émergence des réseaux sociaux et des outils numériques permet donc d'aller plus loin que la création d'un simple double numérique en contribuant au

---

[52] Gérard Haas, Amanda Dubarry, « Confidentialité et protection des données », *Dalloz IP/IT*, 2017, p. 322.
[53] CNIL, *op. cit.*, p. 12.
[54] Yves Deswarte, Sébastien Gams, « Protection de la vie privée : principes et technologies », in *Les technologies de l'information au service des droits : opportunités, défis, limites*, *in* Daniel Le Métayer (éd.), *Cahiers du centre de recherches Information et Droit*, Bruylant, 2010.
[55] Erik H. Erikson, *Adolescence et crise, la quête d'identité*, Paris, éd. Flammarion, coll. "Champs", 1972, 348 p.
[56] Georg Wilhelm Friedrich Hegel, *La phénoménologie de l'esprit*, Paris, Aubier-Montaigne, 1939, 684 p.
[57] Voir notamment : Henri Tajfel, « La catégorisation sociale », *in* S. Moscovici (éd.), *Introduction à la psychologie sociale*, Vol. 1, pp. 272-302, Paris, Larousse, 1972.
[58] François Perea, « L'identité numérique : de la cité à l'écran. Quelques aspects de la représentation de soi dans l'espace numérique », *Les Enjeux de l'Information et de la Communication*, Lavoisier, 2010, vol. 1, p. 144 à 159.
[59] *Ibid.* L'auteur relève également que « l'absence de rencontre directe et l'anonymat ouvrent un espace d'expression accru, qui n'était, dans le monde réel, souvent réservé qu'à des situations clandestines ou secrètes, dans certains milieux interlopes ou clubs privés, et qui maintenant peuvent s'étendre sur le web social et être publicisé à l'infini ».

prolongement de l'identité civile tout en intégrant plus facilement des éléments relatifs à l'intime. Les frontières de cette identité augmentée, devenue aujourd'hui le carburant de l'économie numérique, sont par ailleurs devenues difficile à maîtriser et à délimiter. Comme le révèlent Alain Rallet et Fabrice Rochelandet dans le premier cahier Innovation et Prospective publié par la CNIL en 2012, « le dévoilement de soi est consubstantiel au développement des services marchands web 2.0 ». La transformation des rapports entre individus et acteurs du numérique, au cœur d'une économie de l'immatériel, repose en grande partie sur les annonceurs publicitaires, chargés de monétiser les données obtenues.

26. La projection de soi – Une des conséquences de « la démocratisation des réseaux sociaux est que le partage au sein de ces espaces ne se fait pas totalement au hasard »[60]. Ce *marketing* de soi, comme il est parfois défini[61], incite les individus à se révéler selon l'image qu'ils souhaitent véhiculer. La transmission et le partage d'informations et de données personnelles se fait dès lors en fonction de l'image qu'un individu souhaite renvoyer aux autres. Les modalités de partage des informations obtenues grâce au *quantified-self* sont révélatrices de ce nouveau rapport à l'identité. De plus en plus d'individus ont tendance à partager sur des réseaux sociaux tels que Facebook ou Twitter des éléments relatifs à leur activité physique, le temps réalisé lors d'une course à pieds par exemple ou les progrès réalisés lors d'un régime alimentaire. Outre le bénéfice relatif au bien-être apporté par l'automesure connectée, cet outil favorise la construction de l'image renvoyée par l'individu. Les capacités de partage des données collectées permettent en effet à l'individu de choisir consciemment les éléments qu'il souhaite révéler, participant ainsi à sa construction sociale : l'individu peut orienter la perception que les autres auront de lui. Une personne pourra donc décider de se présenter aux membres de son entourage comme sportive, dynamique et sensible à la question du bien-être. Cette construction numérique du soi questionne le rapport que les individus entretiennent avec la vie privée.

[60] Allain Rallet, Fabrice Rochelandet, *in* CNIL, *op. cit.*, p. 12.
[61] *Ibid.*

La tendance à révéler de plus en plus d'informations ne marque pas la fin de la vie privée car, « plus les individus se dévoilent, plus leur vie privée prend de la valeur : en fait, ils savent gérer la frontière entre ce qu'ils souhaitent exposer et ce qu'ils considèrent comme devant rester intime »[62]. La conception originelle de la vie privée telle que définie par Aristote[63], reposant sur une distinction entre sphère privée et sphère publique, laisserait sa place à « des pratiques qu'il faut appeler privé-public »[64]. Ce n'est dès lors plus simplement la vie privée qui est exposée aux yeux des autres, mais une certaine conception de la vie privée, propre à chaque individu et consciemment travaillée. Ainsi, « façonner sa réputation, animer sa communauté d'admirateurs ou anticiper la viralité de ses messages constitue même un savoir-faire valorisé »[65]. Le web-social s'est ainsi « progressivement couvert de chiffres de petits compteurs, des « gloriomètres » pour reprendre une expression de Gabriel Tarde »[66]. Le *quantified-self* alimente ce modèle et il encourage même la pression sociale de la « normalité » qui pèse sur les individus en mettant à leur disposition des outils de mesure automatisés. Les individus ne peuvent pourtant pas toujours contrôler les modalités de partage de ces informations relatives à l'activité physique, au corps humain ou encore au bien-être. Celles-ci sont transmises aux opérateurs du numérique en charge de les collecter sans parfois pouvoir maîtriser l'utilisation qu'ils en feront ensuite.

27. Le risque informationnel – L'Internet des objets caractérise le passage « d'un réseau d'ordinateurs interconnectés à un réseau d'objets connectés » et son acceptation par la société est « fortement liée au respect de la vie privée et à la protection des données personnelles, deux droits fondamentaux de l'UE »[67]. En effet, la question des risques que les objets connectés font courir aux individus est au cœur des enjeux du sujet : la projection de soi, telle que précédemment évoquée, repose sur une révélation volontaire d'informations de la part des individus. Mais cette révélation est effectuée à la condition que les individus puissent maîtriser à la fois

[62] *Ibid.*
[63] Aristote, *Ethique à Nicomaque*, Flammarion, 1997, 574 p.
[64] Dominique Cardon, « L'identité comme stratégie relationnelle », *Hermès, La Revue*, vol. 53, no. 1, 2009, p. 61 à 66.
[65] Dominique Cardon, *op. cit.*, p. 30.
[66] *Ibid.*
[67] Commission des Communautés Européennes, *L'Internet des objets – un plan d'action pour l'Europe*, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, COM (2009), 278 final, Bruxelles, 18 juin 2009, p. 6.

l'étendue et le spectre des informations qui sont révélées. Or, le déploiement à grande échelle d'objets connectés, associé à la pratique de l'automesure, renforce le risque informationnel qui pèse sur les individus et ce, en dépit d'une réglementation en théorie protectrice des données. Entendu de manière générale comme la perte de maîtrise par les individus des informations qu'ils révèlent aux tiers, ce risque se décompose en deux grandes catégories : l'appréhension d'une information contre la volonté de son détenteur d'une part et la diffusion de fausses informations et d'informations mensongères, que cela soit volontaire ou non d'autre part[68]. L'enjeu est alors de garantir la maîtrise de ce risque informationnel aux individus alors même que les objets connectés constituent « une matière assez nouvelle qui n'est pas encore régie par un ensemble de règles spécifiques »[69].

28. Le juste équilibre entre droits et obligations qui caractérise théoriquement les rapports entre individus et opérateurs du numérique est actuellement remis en question. L'actualité récente est en effet révélatrice des déséquilibres entre individus confiant leurs données à caractère personnel d'une part et entreprises chargées de les traiter et de les analyser d'autre part, considérant notamment « l'opacité qui règne dans « l'économie numérique » et la culture du secret industriel qu'y manifestent les acteurs industriels »[70]. La tendance à l'accroissement quantitatif et qualitatif des possibilités techniques de traitement des données personnelles a en effet atteint un seul critique en termes d'intensité de fichage. Le passage des TIC (Technologies de l'Information et de la Communication) aux NTIC (Nouvelles Technologies de l'Information et de la Communication)[71] confirme que nous sommes aujourd'hui entrés dans l'ère de l'hyperconnexion, révolution semblable à celle de l'imprimerie[72] et le contexte juridique dans lequel évoluent les objets connectés permettant l'automesure nécessite donc d'être envisagé.

---

[68] Thibault du Manoir de Juaye, « Le risque informationnel au filtre du droit », *Documentaliste-Sciences de l'Information*, n° 3, vol. 51, 2014, p. 37 à 40.
[69] Thierry Piette-Coudol, *Les objets connectés, Sécurité juridique et technique*, Lexis Nexis, 2015, p. 21.
[70] Vincent Bullich, Viviane Clavier, « Production des données, « Production de la société ». Les Big Data et algorithmes au regard des Sciences de l'information et de la communication », *Les Enjeux de l'information et de la communication*, Lavoisier, vol. 19/2, no. 2, 2018, p. 5 à 14.
[71] Nicolas Ochoa, *Le droit des données personnelles, une police administrative spéciale*, Thèse pour le doctorat en droit présentée et soutenue publiquement le 8 décembre 2014, Université Paris-I Panthéon-Sorbonne, p. 11.
[72] Laure Marino, « To be or not to be connected : ces objets connectés qui nous espionnent », *Recueil Dalloz*, 2014, p. 29.

II. Le contexte juridique

29. Le profilage algorithmique est une conséquence directe de l'utilisation d'objets connectés dans le cadre de la pratique de l'automesure et celui-ci permet d'influencer directement le bien-être de l'individu mais également sa santé. L'individu peut directement modifier ou adapter son comportement en fonction des informations qui lui sont communiquées par ses dispositifs connectés (faire plus de sport, adapter son rythme de sommeil ou encore son alimentation). Mais l'appropriation et la réutilisation par des tiers à des fins commerciales de telles informations sont également susceptibles d'influencer le comportement des personnes. En effet, le savoir produit par ce profilage peut être appliqué aux individus « de manière à en inférer un savoir ou des prévisions probabilistes quant à leurs préférences, intentions, propensions qui ne seraient pas autrement manifestes »[73].

Les informations personnelles servent de plus en plus à renforcer des normes de comportement et « le traitement de l'information contribue à des stratégies à long terme visant à façonner et ajuster la conduite individuelle »[74]. Ainsi, l'informatisation vient transformer le fragile équilibre sur lequel repose le respect de la vie privée. Or, définir une réglementation permettant d'encadrer solidement ces procédés est essentiel en raison des risques que ceux-ci font courir aux individus[75]. Outre une publicité particulièrement ciblée, le recours à ce type de dispositifs est susceptible d'impacter profondément le quotidien des individus, dans une logique d'évaluation et d'orientation de leurs comportements. Déjà en 2014, un assureur proposait à certains de ses clients un bracelet connecté de type *tracker* d'activité afin de les faire bénéficier de chèques cadeaux en fonction du nombre de pas parcourus dans une journée[76]. A l'heure où certains Etats établissent un système de notation à l'égard de leurs citoyens[77], l'adaptation des polices d'assurance au comportement des individus

[73] Antoinette Rouvroy, Thomas Bern, *op. cit.*, p. 170.
[74] Spiros Simitis, « Reviewing privacy in an information society », *University of Pennsylvania Law Review*, vol. 135, n°3, 1987, p. 710.
[75] Shoshana Zuboff, « Le capitalisme de la surveillance », *Esprit, L'idéologie de la Silicon Valley*, n° 454, mai 2019, p. 75.
[76] Geoffray Sylvain, « AXA conditionne un avantage santé à un objet connecté », Aruco, 3 juin 2014, disponible en ligne à cette adresse : https://aruco.com/2014/06/axa-objet-connecte/
[77] Elsa Trujillo, « La Chine commence déjà à mettre en place son système de notion des citoyens prévu pour 2020 », Le Figaro, 27 décembre 2017, accessible en ligne à cette adresse : http://www.lefigaro.fr/secteur/high-tech/2017/12/27/32001-20171227ARTFIG00197-la-chine-met-en-place-un-systeme-de-notation-de-ses-citoyens-pour-2020.php

relevés dans le cadre de l'automesure connectée serait particulièrement susceptible de nuire aux droits des individus, droit au respect de la vie privée notamment.

30. Une proposition de loi visant à interdire l'usage des données personnelles collectées par les objets connectés dans le domaine des assurances a ainsi été enregistrée à la Présidence de l'Assemblée nationale le 23 janvier 2019[78]. Rappelant l'intérêt d'outils permettant « d'auto-enregistrer toute une série de données liée soit au mode de vie, soit au bien-être, soit plus généralement à l'état de santé de l'utilisateur »[79], cette proposition de loi vise à interdire l'usage des données collectées dans un domaine qui repose traditionnellement sur deux mécanismes essentiels : confiance entre assurés et assureurs d'une part et mutualisation d'autre part[80]. La réutilisation par des assureurs de données collectées dans le cadre de l'automesure pour ajuster leurs politiques tarifaires fausserait cette relation de confiance car elle viserait à écarter toute forme d'aléa, propre à la réalisation éventuelle d'un risque.

Cet exemple relatif à l'utilisation des données personnelles issues de l'automesure en matière de polices d'assurance est révélateur des enjeux soulevés par le sujet. Celui-ci pose naturellement la question de l'appréhension par le droit des risques que font courir des traitements de données à grande échelle aux individus. Mais il est également révélateur de l'influence que le numérique est susceptible d'avoir sur la création des normes.

A. La création des normes influencée par le numérique

31. Le droit à la protection des données à caractère personnel a connu, au cours de l'année 2018, une actualité sans précédent. L'entrée en application le 25 mai 2018 du Règlement général sur la protection des données (RGPD) adopté en 2016[81] a permis de mettre en lumière les problématiques relatives à la question de la protection des informations des individus. Cette réforme d'ensemble du système de protection des données était ainsi attendue depuis 2012, date à laquelle une directive avait été

[78] Proposition de loi visant à interdire l'usage des données personnelles collectées par les objets connectés dans le domaine des assurances, enregistré à la Présidence de l'Assemblée nationale le 23 janvier 2019.
[79] *Ibid.*
[80] CNIL, *Le corps, nouvel objet connecté, Du quantified-self à la M-Santé : les nouveaux territoires de la mise en données du monde, op. cit.*, p. 37.
[81] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

proposée par Viviane Reding. L'outil du règlement a finalement été retenu et son adoption s'est inscrite dans un contexte particulier de défiance envers les Etats et les entreprises du numérique. En effet, les informations dévoilées par Edward Snowden en juin 2013 ont profondément impacté les questions relatives à la surveillance de masse ainsi qu'à la vie privée et à la protection des données des individus. Ces révélations, relatives à la surveillance des communications opérées par la National Security Agency (NSA), agence de renseignement américaine, en lien avec des grandes entreprises d'Internet, ont eu pour effet d'instaurer un climat de méfiance envers celles-ci et tout particulièrement envers les GAFAM (Google, Amazon, Facebook, Apple, Microsoft).

32. Outre cette problématique relative à la surveillance, les failles de sécurité et autres piratages ayant touché certains services[82], dont certains particulièrement sensibles[83], ont également contribué aux débats relatifs aux enjeux de la protection des données. Les statistiques réalisées sur la confiance des internautes envers les services utilisant leurs données à caractère personnel sont à ce titre particulièrement révélatrices. En effet, 74% des français estiment ne pas avoir confiance dans les applications mobiles quant à l'utilisation qui est faite de leurs données[84] et près de deux tiers des utilisateurs mondiaux seraient méfiants envers une utilisation par les applications mobiles de ces mêmes informations[85]. Pourtant, l'environnement dans lequel se tissent les liens entre utilisateurs de services en ligne et fournisseurs desdits services, qualifié de *web symbiotic*, contribue nécessairement à la révélation d'informations par les individus. Le traitement de données à caractère personnel est ainsi inéluctable, « car celui qui prétendrait s'y soustraire se placerait en dehors de la vie sociale telle qu'elle est aujourd'hui organisée »[86].

33. La singularisation du droit à la protection des données personnelles – Droit au respect de la vie privée et protection des données à caractère personnel, bien

[82] La chaîne de magasin américaine Target a ainsi été victime, entre novembre et décembre 2015, d'une cyber-attaque touchant près de 40 millions de clients.
[83] Le site de rencontre adultère Ashley Madison a fait l'objet en juillet 2015 d'un piratage touchant près de 33 millions de comptes.
[84] Sophie Eustache, « Données personnelles : 3/4 des Français ne font pas confiance aux applis mobiles », *L'Usine Digitale*, 21 avril 2016.
[85] KPMG, *Crossing the line : staying on the right side of consumer privacy*, 2016, p. 7.
[86] Guillaume Desgens-Pasanau, « Informatique et libertés, une équation à plusieurs inconnues », *in* Jean-Luc Girot (dir.), *Le harcèlement numérique*, Dalloz, 2005, p. 97.

que souvent rapprochés[87], sont deux notions historiquement et conceptuellement différentes. En effet, si « certaines tensions les rapprochent dans une problématique globale du privé à l'ère du numérique »[88], ces deux droits ne se confondent pas. Le droit à la protection de la vie privée, identifié à la fin du XIXème siècle comme un droit à être « laissé tranquille »[89] a progressivement évolué pour être entendu de manière contemporaine comme la revendication des individus à pouvoir déterminer selon quelles modalités les informations les concernant sont révélées[90]. Ainsi, le droit au respect de la vie privée ne consiste pas simplement à devenir totalement invisible aux yeux des autres, mais il implique surtout une capacité de contrôle des individus sur les informations les concernant[91]. La notion de droit au respect de la vie privée, malgré son affirmation dès 1948 au sein de la Déclaration universelle des droits de l'Homme, n'a été insérée qu'en 1970 au sein de l'article 9 du Code civil qui dispose que « chacun a droit au respect de sa vie privée ». Considéré comme un des aspects de la dignité de la personne[92], le droit au respect de la vie privée s'est présenté comme un terreau fertile et propice au développement d'une réglementation propre aux données à caractère personnel des individus. Celle-ci est aujourd'hui remise en question par des technologies de l'information et de la communication toujours plus performantes.

34. Un droit en pleine mutation – Réglementer de façon pérenne la mise en œuvre de traitements de données à caractère personnel est une tâche particulièrement complexe. Les législateurs nationaux et européens sont en effet confrontés à un secteur en constant mouvement. La permanence des évolutions technologiques rend difficile l'adoption d'une législation permettant d'encadrer avec pertinence et sur le long terme les risques auxquels sont soumis les individus. Il n'est pas possible de prévoir avec exactitude les évolutions de l'informatique, entendue comme la science du traitement rationnel de l'information par machines automatiques[93]. Les premiers

[87] La directive 95/46/CE mentionne par exemple dans son considérant 10 que « l'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit à la vie privée ».
[88] Bénédicte Rey, *La vie privée à l'ère du numérique*, Lavoisier, 2012, 304 p.
[89] Samuel Warren, Louis Brandeis, « The right to privacy », *Harvard Law Review*, vol. IV, 193, Dec. 15, 1890.
[90] Alan F. Westin, Daniel J. Solove, *Privacy and freedom*, Athenum, New York, 1967.
[91] Charles Fried, « Privacy », *The Yale Law Journal*, Vol. 77, n°3, January 1968, p. 475 à 493.
[92] Edward J. Bloustein, « Privacy as an Aspect of Human Dignity », *New York University Law Review*, 1964, n° 39, p. 962 à 1007.
[93] Bulletin Officiel de l'Education Nationale, 26 février 1981, n° 8.

éléments de législation, adoptées dans le courant des années 1970, ont ainsi dû faire face au nombre croissant d'ordinateurs au sein des foyers, à leur connexion progressive à Internet ainsi qu'à leur miniaturisation avec l'apparition des *smartphones*. Le développement des réseaux sociaux et enfin, la connexion à Internet d'objets du quotidien, ont par ailleurs marqué l'avènement de l'ère des traitements instantanés de données à caractère personnel. Les différents textes initialement adoptés ont donc dû progressivement être adaptés à ces évolutions technologiques. Ceux-ci ont néanmoins réussi à faire preuve d'une étonnante capacité d'adaptation en adoptant une approche fondée sur le traitement lui-même plutôt que sur le dispositif utilisé pour y parvenir.

1. Un mouvement législatif européen généralisé

35. Les problématiques relatives à la création et à l'utilisation de fichiers informatiques sont apparus de façon simultanée au niveau européen et mondial. Déjà en 1974, un *Privacy Act* adopté aux Etats-Unis visait à établir des règles à l'égard des traitements de données effectués par les différentes branches et agences du gouvernement fédéral américain. Le développement généralisé de l'informatique au sein des administrations a justifié qu'un mouvement convergent de législation soit également adopté au niveau des différents Etats européens. Ce mouvement législatif s'est caractérisé par l'adoption de cadres généraux de protection, à la différence de ceux sectoriels ayant déjà pu voir le jour[94]. Le droit français apparaît comme pionnier et « la France constitue un des premiers Etats au monde, et le premier Etat membre des Communautés économiques européennes, à avoir adopté dans son droit positif une telle réglementation »[95]. Bien que pionnier, le mouvement législatif français ayant conduit à l'adoption d'un cadre général de protection des informations nominatives (a) a également été précédé ou suivi de l'adoption de différentes mesures similaires par les différents Etats européens (b).

[94] Voir notamment la loi n°70-539 du 24 juin 1970 concernant la centralisation de la documentation relative à la circulation routière, JORF du 25 juin 1970, p. 5963.
[95] Nicolas Ochoa, *op. cit*., p. 25.

a. En France

36. La loi Informatique et Libertés. Le cadre général français de protection des données à caractère personnel est contenu au sein de la loi du 6 janvier 1978, dite loi relative à l'informatique, aux fichiers et aux libertés (LIL). Désormais quarantenaire et bien qu'ayant fait l'objet de différentes réformes[96], l'objectif de cette loi est aujourd'hui toujours le même : garantir les libertés des individus à l'égard de l'utilisation de l'informatique. Celle-ci vise précisément à réglementer la mise en œuvre de traitements de données à caractère personnel, informations nominatives permettant d'identifier directement ou indirectement les individus, tout en conférant certains droits aux individus concernés par de tels traitements et en mettant certaines obligations à la charge des personnes responsables de tels traitements. Cette répartition est encore d'actualité aujourd'hui mais elle a progressivement changé d'objectifs. L'équilibre entre droits et obligations visait initialement à assurer la protection des individus à l'égard des administrations constituant des fichiers. Désormais, celui-ci vise à assurer la protection des individus à l'égard des administrations mais aussi et peut-être surtout, à l'égard des entreprises privées procédant à des traitements de données pour les besoins de leurs services.

37. La protection contre les traitements réalisés par les administrations. La loi de 1978 avait à l'origine pour objectif de protéger les individus des traitements de données réalisés par les personnes publiques[97]. L'adoption de cette loi était en effet justifiée à l'époque par les révélations du quotidien *Le Monde* relatives au projet dit SAFARI (Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus) d'interconnexion de différents fichiers administratifs nominatifs[98]. La polémique qui a suivi la parution de cet article a permis à cette thématique d'émerger dans le débat public et politique. Une commission Informatique et Libertés a ainsi été créée, pour proposer des éléments de réglementation quant à l'utilisation de l'informatique et des données des individus. Créée par le décret n°74-938 du 8

[96] La dernière version de cette loi, portant adaptation du cadre juridique national aux évolutions engendrées par le Règlement général européen est entré en vigueur en juin 2018 et celle-ci a fait l'objet d'une réécriture complète par l'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018.
[97] Vivian Laugier, « La confiance dans l'administration à l'ère du numérique : l'exemple du traitement des données à caractère personnel », *in* Catherine Teitgen-Colly, Olivier Renaudie (dir.), *Confiance et droit public*, L'Harmattan, coll. Logiques Juridiques, 2019, 288 p.
[98] Philippe Boucher, « SAFARI ou la chasse aux Français », *Le Monde*, 21 mars 1974.

novembre 1974, cette commission avait à l'origine pour but de « proposer au Gouvernement […] des mesures tendant à garantir que le développement de l'Informatique, dans les secteurs publics, semi-public et privé se réalisera dans le respect de la vie privée, des libertés individuelles et des libertés publiques »[99]. Surtout, « instrument très majoritairement aux mains de l'Etat en raison de son coût à l'époque, l'informatique, au travers de cette représentation, a ainsi cristallisé les contestations latentes ou exprimées d'un pouvoir étatique perçu comme menaçant pour la société et l'individu »[100]. Cette commission deviendra, avec la loi du 6 janvier 1978, la Commission nationale de l'Informatique et des Libertés.

Le rapport déposé le 27 juin 1975 par la Commission et dont la paternité est attribuée à Bernard Tricot, conseiller d'Etat et rapporteur général, ouvrira la voie à l'adoption, trois ans plus tard, de la loi Informatique et Libertés du 6 janvier 1978[101]. Ce rapport relève à l'époque que « dans l'état actuel des choses, l'informatique est plus naturellement à disposition des puissants qu'à celle des faibles », permettant de justifier que ses « utilisateurs privilégiés sont donc l'Etat, les grandes villes, les entreprises publiques, les banques et les assurances, les grandes entreprises privées, les groupements politiques et professionnels les plus puissants »[102]. Comme le révèle déjà le rapport rédigé par le sénateur Jacques Thyraud lors des débats suivant l'adoption du projet de loi par l'Assemblée Nationale, « les vrais problèmes, en fait, que pose le traitement automatisé des informations sont des problèmes de collecte des données et d'utilisation de ces mêmes données »[103]. La raison d'être du texte n'était donc pas de limiter les développements de l'informatique mais plutôt d'en encadrer l'utilisation dans le but de protéger les individus contre d'éventuelles utilisations abusives de leurs données, entendues comme des informations nominatives permettant de les identifier.

38. Une recherche de pérennité. L'idée sous-jacente à la rédaction du texte était de « ne pas mettre l'informatique en position d'accusée mais au contraire,

[99] Décret n°74-938 du 8 novembre 1974 portant création de la commission Informatique et libertés, article 1er.
[100] Nicolas Ochoa, *op. cit*., p. 30.
[101] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[102] Rapport de la Commission Informatique et Libertés, *La Documentation française*, 27 juin 1975, p. 17.

d'essayer de mesurer l'ampleur du phénomène qu'elle représente avant de la réglementer »[104]. Le législateur a par ailleurs dû, lors de l'élaboration de la loi, faire face au caractère évolutif et technique du secteur devant faire l'objet d'une régulation : fallait-il encadrer précisément la mise en œuvre de traitements de données, en prenant en compte les éléments techniques employés ? A ce titre, si « l'opinion générale a été que l'excès de réglementation se traduisait souvent par son inapplicabilité », le législateur a cherché à « faire des lois les plus générales et les plus claires possibles afin de permettre, dans l'application, une certaine souplesse »[105]. De la prise en compte de cette spécificité relative au caractère technique du numérique dépendait la pérennité du texte adopté et son adaptabilité à l'émergence de nouvelles technologies.

L'article 1er du texte dispose que « l'informatique doit être au service de chaque citoyen ». La loi adoptée en 1978, « loi de libertés publiques qui fixe une finalité au développement de l'informatique »[106], garantit la protection des droits et libertés des individus. Pour y parvenir, elle encadre et réglemente la mise en œuvre des traitements automatisés d'informations nominatives. Ainsi, alors que « le droit public a été utilisé pour aménager un régime original de libertés publiques comme parade aux menaces que l'informatique pourrait faire peser sur la vie privée, tant dans le secteur privé que dans le secteur public »[107], un régime de formalités préalables auprès d'une autorité administrative indépendante est mis en œuvre par le texte et les individus disposent dans le même temps d'un droit d'accès à leurs données personnelles. Pourtant, l'objet de cette loi « n'est pas la seule réglementation des informations nominatives » puisque « comme le montrent clairement ses trois premiers articles, elle aborde le problème des rapports entre l'informatique et les libertés dans sa perspective la plus large »[108]. A ce titre, l'individu est également

---

[103] Jacques Thyraud, *Rapport fait au nom de la Commission des Lois constitutionnelles, de Législation, du Suffrage universel, du Règlement et d'Administration générale, sur le projet de loi, adopté par l'Assemblée Nationale, relatif à l'informatique et aux libertés*, Sénat, Première session ordinaire de 1977-1978, n° 72, p. 8.
[104] *Ibid.*, p. 16.
[105] *Ibid.*
[106] Herbert Maisl, « Etat de la législation française et tendances de la jurisprudence relatives à la protection des données personnelles », *Revue Internationale de Droit comparé*, n°3, 1987, p. 559 à 580.
[107] *Ibid.*
[108] CNIL, *Bilan et perspectives 1978-1980, Premier Rapport au Président de la République et au Parlement*, La Documentation Française, 1980, p. 9.

protégé envers d'éventuelles décisions de justice ou administratives fondées sur un traitement automatisé d'informations et « donnant une définition du profil ou de la personnalité de l'intéressé », sachant que lorsque des résultats fondés sur des traitements automatisés lui sont opposés, l'individu « a le droit de connaître et de constater les informations et les raisonnements utilisés »[109]. Le système de protection instauré en 1978 repose donc majoritairement sur l'information de l'individu et sur sa possibilité de s'opposer aux traitements informatisés mis en œuvre.

39. Le RGPD. Aujourd'hui, le Règlement général européen entré en vigueur en 2018 renouvelle les obligations pesant sur les personnes publiques. A titre d'exemple, la désignation d'un délégué à la protection des données, ancien correspondant Informatique et Libertés, est désormais obligatoire lorsque « le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle »[110]. Cette désignation était auparavant simplement facultative mais elle devient désormais obligatoire avec le nouveau texte européen. Le recours à un délégué à la protection des données, investi d'une mission de conseil mais également de contrôle du respect des dispositions relatives à la protection des données à caractère personnel, est révélateur des capacités de traitement donc disposent également aujourd'hui les administrations. La transformation numérique de l'action publique, associée aux craintes relatives à la surveillance étatique de masse, justifie à certains égards qu'un tiers soit chargé de contrôler le respect de la réglementation par ces entités. Cependant, la vague de modernisation amorcée par la directive de 1995 est majoritairement justifiée par l'accroissement exponentiel des capacités de traitement à disposition des entreprises privées.

40. La protection contre les traitements réalisés par les entreprises. Les éléments de réglementation adoptés en France à la fin des années 1970 avaient pour vocation première de protéger les individus contre les traitements de données à caractère personnel et les interconnexions de fichiers réalisés par les administrations. Celles-ci détenant à l'époque l'essentiel du parc informatique, « les mesures

[109] Articles 2 et 3, loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[110] Article 37, Règlement (UE) 2016/679.

législatives adoptées […] avaient donc pour objet premier de protéger le citoyen contre les dérives policières auxquelles la mise en œuvre de traitements centralisés et l'exploitation systématique de données personnelles pouvaient conduire les principales administrations publiques »[111]. Ainsi, les enjeux relatifs au développement du numérique et à l'apparition d'outils informatiques en réseaux étaient initialement associés aux éventuelles intrusions dans la sphère privée réalisées par des organismes publics. Pourtant et progressivement, ces données de base ont été profondément modifiées par le développement de la micro-informatique, par sa très large diffusion dans les entreprises et auprès des particuliers. L'informatique s'est en effet banalisée à ce moment, au point de devenir indispensable à l'essentiel des activités courantes. Les entreprises privées ont donc progressivement eu recours de façon généralisée à l'informatique, ces opérateurs économiques s'appuyant largement sur les données à caractère personnel des individus pour développer leurs services.

La constitution de bases de données à caractère personnel par les entreprises a constitué une évolution notable des activités commerciales, permettant notamment un développement de la publicité dite ciblée et marquant la personnalisation des offres proposées. Dès lors, ces bases de données ont constitué un marché à part entière et leur constitution et leur traitement a été l'élément principal de la valeur ajoutée produite par un grand nombre d'entreprises de services. Ce changement de paradigme a ainsi entériné la limitation du champ du monopole des opérateurs publics sur certaines bases de données, au bénéfice des opérateurs privés.

L'adoption de la directive 95/46/CE a donc marqué la volonté de garantir la liberté des échanges d'informations entre les différents Etats membres, tout en garantissant le respect des droits des individus. Surtout, ce texte a tenu à éviter toute concurrence potentielle fondée sur des niveaux de protection différents des droits reconnus aux individus entre Etats membres. L'un des principaux défis posés au législateur français lors de la transposition de la directive de 1995 a ainsi été de mettre sur un pied d'égalité les secteurs publics et privés, les fichiers publics étant traditionnellement plus réglementés que les fichiers privés.

[111] Guy Braibant, *Données personnelles et société de l'information*, Rapport au Premier Ministre sur la transposition en droit français de la directive n°95/46, 3 mars 1998, p. 1.

41. La loi de transposition de la directive de 1995, entrée en application en 2004[112], a constitué la première vraie réforme d'ampleur de la loi Informatique et Libertés de 1978. Celle-ci a dû prendre en compte le changement d'origine des traitements de données à caractère personnel, des organismes publics aux entreprises privées. Les formalités préalables à la mise en œuvre d'un traitement de données ont ainsi été modifiées. En effet, alors que dans le système originaire, les traitements des services publics étaient soumis à autorisation et que les traitements privés étaient soumis à déclaration auprès de l'autorité administrative indépendante, selon un critère organique, celui-ci a été remplacé par un critère horizontal, soumettant à un examen préalable les « traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées »[113]. Ainsi, les traitements automatisés d'informations nominatives opérés pour le compte de l'Etat, d'un établissement public ou d'une collectivité territoriale ou d'une personne morale de droit privé gérant un service public étaient décidés par une loi ou par un acte réglementaire pris après avis de la CNIL. Les autres traitements devaient simplement faire l'objet d'une déclaration préalable auprès de cette même commission, celle-ci étant tenue de délivrer un récépissé[114]. La gradation des formalités préalables à mettre en œuvre ne dépendait dès lors plus de la nature juridique de l'entité à l'origine du traitement, mais du degré de risque que celui-ci était susceptible de faire naître à l'égard de l'individu. La transposition de la directive a donc permis de mettre fin à la distinction qui était auparavant faite par les articles 15 à 17 de la version initiale de la loi Informatique et Libertés distinguant les traitements publics et privés. Ce critère organique n'a pourtant pas disparu et il est encore utilisé aujourd'hui, en raison notamment de la spécialisation croissante des traitements opérés[115].

b. En Europe

42. Les éléments de réglementation relatifs à la protection des données à caractère personnel dont s'est dotée la France à la fin des années 1970 s'inscrivent dans un mouvement européen plus général de prise en compte de ces problématiques.

---

[112] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[113] Article 20, directive 95/46/CE du 24 octobre 1995.
[114] CE, 6 janvier 1997, *Caisse d'épargne Rhône-Alpes Lyon c. CNIL*, n° 159129, publié au recueil Lebon.
[115] *Cf.*, *infra*, n° 547.

La généralisation du recours à l'informatique au sein des administrations, l'apparition de questions relatives à la surveillance des administrés ainsi que la transformation numérique progressive des services commerciaux ont suscité, en Europe, l'émergence progressive d'un certain nombre de réglementations aux objectifs similaires. La France fait partie des premiers Etats à s'être doté d'une législation spécifique à la protection des données à caractère personnel, après le land d'Hesse en Allemagne en 1970[116] et la Suède en 1973[117]. Le caractère transversal des traitements de données à caractère personnel réalisés, leur internationalisation ainsi que leurs transferts entre plusieurs Etats ont pu bénéficier du développement, au sein des Etats européens, de ces différentes règles protectrices. L'adoption de textes spécifiques à la question des données personnelles marque le début d'une première vague de réglementation, qui s'étend de 1970 à 1981, date de l'adoption de la Convention n°108 du Conseil de l'Europe. Deux modèles distincts de réglementation ont ainsi été adoptés : des dispositions législatives *ad hoc* et des dispositions de nature constitutionnelle.

43. La consécration législative. Les années 1970 virent l'éclosion d'un ensemble de législations nationales relatives à la protection des données à caractère personnel. Les différents Etats concernés adoptèrent ainsi des mesures visant à encadrer la démocratisation de l'informatique, notamment au sein des administrations, en respectant leurs différentes traditions juridiques. Le land d'Hesse a été le premier à adopter un instrument spécifiquement dédié à cette matière, avec un champ d'application initialement limité aux informations du secteur public[118]. Outre des codes de conduite destinés aux administrations, l'acte adopté conférait certains droits aux individus, droit de rectification des informations collectés notamment. Par ailleurs, cet acte cherchait également à protéger les individus contre d'éventuels accès malveillants de tiers à leurs informations. Cette protection a été encouragée par le recours à un commissaire à la protection des données, chargé de la mise en œuvre de contrôle au sein des institutions et de l'observation des effets de la transformation numérique dans les rapports entre celles-ci[119]. Le législateur suédois contribuera par la suite à la mise en œuvre de la première législation nationale relative à la protection

[116] Hessian Data Protection Act of Oct. 7, 1970.
[117] Swedish Data Protection Law of May II, 1973, *Datalagen*.
[118] Fritz Hondius, *Emerging Data Protection in Europe,* Amsterdam : North-Holland Publishing Company, 1975, p. 36.
[119] *Ibid.*, p. 36.

des données. Adopté le 11 mai 1973, ce *Datalag* met en balance différents intérêts relatifs notamment à l'utilisation croissante de l'informatique au sein des administrations et à la protection des droits des individus. A l'image de ce qui avait été mis en place par le land d'Hesse, le système de protection suédois procéda à la création d'une autorité chargée de contrôler la mise en œuvre de traitements de données[120]. Le processus législatif permettant l'adoption de lois protectrice des données s'est par la suite répandu avec l'adoption de textes au Danemark, en Norvège et au Luxembourg et il a également fait son apparition au sein de différentes constitutions d'Etats européens.

44. La consécration constitutionnelle. A la différence d'Etats ayant adopté des dispositifs d'ordre simplement législatif, d'autres pays européens ont préféré procéder à une constitutionalisation de certains des éléments de réglementation établis. La Constitution portugaise de 1976 consacre ainsi son article 35 à l'utilisation des données à caractère personnel. Premier Etat européen à introduire ce type d'éléments au sein de sa Constitution, le Portugal a ouvert la voie à la constitutionnalisation des questions relatives à l'utilisation et à la protection des données des individus. Trois éléments de protection ont ainsi été consacrés : droit à l'information des individus, interdiction du traitement des données sensibles ou encore interdiction d'utiliser un identifiant unique pour croiser des données. L'Autriche et l'Espagne font également partie des Etats ayant érigés le droit à la protection des données à caractère personnel en droit ayant une valeur constitutionnelle. Les problématiques relatives à la constitutionnalisation du droit à la protection des données à caractère personnels sont révélatrices de l'influence que les nouvelles technologies ont sur l'ordonnancement juridique des normes d'un Etat, y compris au plus haut niveau.

En France, le silence de la Constitution tranchait jusqu'à maintenant avec « l'abondance des consécrations du droit au respect de la vie privée dans les textes contemporains internes comme internationaux »[121]. A l'origine, la rencontre entre Internet et la Constitution, bien qu'inéluctable, marquait la volonté de faire d'Internet

[120] *Ibid.*, p. 38.

un espace de liberté, mais non un espace de non-droit[122]. La protection constitutionnelle, fondée à l'origine sur la reconnaissance par le Conseil constitutionnel d'un principe de respect de la vie privée, a d'abord été jugée suffisante pour garantir l'encadrement de cette liberté. Pourtant, la singularisation progressive du droit à la protection des données a fait que le fondement du respect de la vie privée n'a plus semblé être adapté à l'ensemble des questions relatives à la protection des données. La nécessité de consacrer un fondement constitutionnel spécifique s'est donc manifestée, notamment pour préserver efficacement les droits et libertés du citoyen[123].

La question de la constitutionnalisation du droit à la protection des données à caractère personnel a dès lors également été envisagée en France et les députés ont voté en 2018 l'inscription de cette protection au sein de l'article 34 de la Constitution[124]. Plusieurs décisions rendues par le Conseil constitutionnel entre 2017 et 2018 ont par ailleurs confirmé « le rapprochement entre les standards constitutionnels et européens de protection des données à caractère personnel », tout en témoignant d'un « renforcement du contrôle du juge constitutionnel quant aux possibles atteintes aux données à caractère personnel qui peuvent être commises, tant sur le terrain du traitement automatisé de ces données que sur celui du recueil des données de connexion »[125]. Le Conseil constitutionnel a progressivement intégré ces problématiques, par le biais notamment du fondement de la liberté proclamé à l'article 2 de la Déclaration des droits de l'homme et du citoyen, étendu par ailleurs à « la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel »[126]. A l'image du contrôle opéré par la Cour Européenne des droits de l'Homme lorsqu'un traitement est mis en œuvre à des fins

---

[121] Vincent Mazeaud, « La constitutionnalisation du droit au respect de la vie privée », *Nouveaux Cahiers du Conseil Constitutionnel*, n°48, 2015, p. 7.
[122] Isabelle Falque-Pierrotin, « La Constitution et l'Internet », *Les nouveaux cahiers du Conseil constitutionnel*, 2012/3, n° 36, pp. 31-44.
[123] Marie-Charlotte Roques-Bonnet, *La Constitution et l'Internet*, thèse de droit public, Université Toulouse-I Capitole, 2008.
[124] Le Monde, « L'assemblée inscrit la « protection » des données personnelles dans la Constitution, 19 juillet 2018, accessible en ligne à cette adresse : https://www.lemonde.fr/pixels/article/2018/07/19/l-assemblee-inscrit-la-protection-des-donnees-personnelles-dans-la-constitution_5333463_4408996.html
[125] Nina Le Bonniec, « Vers une convergence des exigences constitutionnelles et européennes en matière de protection des données personnelles numériques ? », *La Semaine Juridique*, Edition Générale, n° 23, 4 juin 2018, p. 1129.
[126] CC, Décision n° 2012-652 DC du 22 mars 2012, *Loi relative à la protection de l'identité*, considérant 8.

de sécurité publique, le Conseil considère que « la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif »[127]. Le juge constitutionnel français semble donc aujourd'hui désireux de garantir efficacement les droits des individus à l'égard des traitements des données à caractère personnel.

2. Un mouvement législatif européen harmonisé

45. L'adoption par un certain nombre d'Etats de législations spécifiques permettant de protéger les individus à l'égard des traitements de données à caractère personnel a permis la mise en lumière de ces problématiques au niveau européen. Mais ce mouvement a également été porteur de risques, l'adoption de textes par des Etats aux traditions juridiques parfois différentes a laissé craindre l'apparition de divergences entre ces différentes législations. Celles-ci auraient pu entraver, sur le long terme, la libre circulation des informations, ainsi que les échanges commerciaux entre les différents Etats membres. L'idée d'établir une directive encadrant de façon harmonisée le droit à la protection des données à caractère personnel a dès lors vu le jour. La directive, finalement adoptée en 1995, est devenue le socle commun de la protection des données en Europe et elle a permis d'harmoniser les cadres juridiques nationaux. Cette évolution s'est poursuivie avec l'adoption du Règlement général européen sur la protection des données entraînant en France la réécriture de la loi Informatique et Libertés de 1978.

a. La construction progressive d'un droit communautaire

46. Le considérant 11 de la directive de 1995 précisait que celle-ci avait pour objectif d'établir une « protection équivalente de haut niveau dans tous les Etats membres de la Communauté afin d'éliminer les obstacles aux échanges de données nécessaires au fonctionnement du marché intérieur ». Le texte européen a notamment dû composer avec des traditions juridiques opposées, entre Etats souhaitant une réglementation détaillée d'une part et Etats souhaitant simplement l'établissement de lignes directrices. La directive a finalement laissé une grande marge de manœuvre

[127] CC, Décision n°2017-637 QPC du 16 juin 2017, *Assoc. Nationale des supporters.*

aux Etats quant à la transposition dans leur droit interne des dispositions du texte européen, sachant que la motivation principale du texte était de favoriser la liberté de circulation des informations. Cet objectif de réalisation du marché intérieur, renforcé par liberté de circulation des informations, a dû être concilié avec la nécessité de protéger les droits des individus à l'égard de leurs données à caractère personnel.

47. La genèse – L'idée d'établir un cadre européen harmonisé de protection s'est rapidement imposée. La généralisation du recours à l'informatique dans les administrations ainsi que le développement d'Internet sous sa forme actuelle ont en effet justifié de repenser cette question. L'éclosion de nouveaux services numériques, notamment commerciaux, le développement de la publicité en ligne ainsi que les modalités renouvelées de transferts de données entre différents Etats sont autant d'éléments ayant justifié d'appréhender de façon globale et à un échelon communautaire la question de la régulation des traitements de données. La Convention 108 du Conseil de l'Europe ouverte à la signature le 28 janvier 1981, premier instrument juridique international contraignant dans le domaine de la protection des données, a semblé être à l'époque un instrument protecteur satisfaisant. Son adoption permet notamment d'expliquer l'absence d'urgence à adopter un texte européen de portée générale, malgré un certain nombre de travaux préparatoires réalisés dès le milieu des années 1970.

Une résolution du Parlement européen, adoptée en 1975, évoquait déjà la nécessité d'adopter une directive permettant la protection des droits et libertés des individus à l'égard des traitements automatisés de données[128]. Suivies d'une seconde résolution un an plus tard[129], ces initiatives n'ont pas trouvé d'échos au sein de la Commission ou du Conseil, en dépit des risques de voir apparaître des divergences entre les différentes législations nationales adoptées par les Etats membres. Le Parlement européen poursuivit ses travaux et adopta une troisième résolution en mai 1979[130]. Celle-ci prenait notamment acte de l'adoption, par les différents Etats

[128] Resolution of the European Parliament on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing [1975] OJ C60/48.
[129] Resolution of the European Parliament of 8 April 1976 on the protection of the right of the individual in the face of developing technical progress in the field of automatic data processing, OJ [1976] OJ C100/27.
[130] Resolution of the European Parliament on the protection of the rights of the individual in the face of technical developments in data processing [1979] OJ C140/34.

membres, de textes relatifs à la protection des données à caractère personnel des individus. Surtout, cette résolution mettait l'accent sur l'éventuel impact négatif que des dispositions nationales contraires ou divergentes pourraient avoir sur le développement d'un marché commun du traitement des données. Une quatrième résolution de mars 1982 enjoignant aux Etats membres de ratifier la Convention n°108 confirma la pertinence de celle-ci, bien qu'un projet de texte commun ne fût pas abandonné en raison de la croissance exponentielle des traitements internationaux de données[131].

L'adoption en 1990 de propositions relatives à la protection des données à caractère personnel, sous la forme d'une communication de la Commission[132], peut être considérée comme « l'élément clef »[133] ayant permis l'adoption d'un texte commun. Cette communication, tout en notant les disparités existantes entre les différentes législations nationales, notamment quant aux conditions de mise en œuvre de traitements de données à caractère personnel, posa les bases de ce que devait être le première texte commun. Surtout, elle permettait de mettre fin aux hésitations observées jusque-là et résultant de la difficulté à établir un texte commun visant à réglementer un objet technologique nouveau et mouvant.

48. La directive – Le texte adopté après de nombreuses modifications[134] le 24 octobre 1995 se différenciait des réglementations nationales édictées jusqu'alors. Notamment, l'adoption de ce texte était justifiée par la nécessité de favoriser la libre circulation des données tout en mettant en place un marché unique d'échange d'informations. Ce texte ne consacrait pas explicitement un droit à la protection des données à caractère personnel mais visait en revanche à établir une protection des personnes physiques à l'égard du traitement des données à caractère personnel[135]. Il ne s'agissait donc pas de doter directement les individus d'outils juridiques leur

[131] Resolution of the European Parliament of 9 March 1982 on the protection of the rights of the individual in the face of technical developments in data processing [1982] OJ C87/39.
[132] COM (90) 314 final.
[133] Gloria Gonzalez, *op. cit.*, p. 124.
[134] Voir notamment la proposition de directive révisée en 1992 : 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 (92/C 311/04), COM (92) 422 final—SYN 287, submitted by the Commission on 16 October 1992 [1992] OJ C311.
[135] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

permettant de protéger leurs informations identifiantes, mais plutôt d'organiser les modalités selon lesquels celles-ci pouvaient être collectées, transférées et échangées.

Un équilibre a dû être établi entre d'une part, la nécessité que « des données à caractère personnel puissent circuler librement d'un Etat membre à l'autre » et d'autre part, la nécessité que « les droits fondamentaux des personnes soient sauvegardés »[136]. A l'image des dispositions de la Convention n°108, la directive de 1995 visait à établir un cadre vertueux et protecteur favorisant les transferts internationaux de données. Pour y parvenir, un certain nombre de critères encadrant les opérations de collecte et de traitement de données ont été mis en œuvre, ceux-ci étant plus contraignants que ceux jusqu'à présent déterminés par les législations nationales. Surtout, le consentement de l'individu a été placé au cœur du dispositif protecteur et a permis de justifier la mise en œuvre de traitements de données à caractère personnel.

Conformément à l'article 1.2 de la directive, les Etats ne pouvaient « restreindre ni interdire la libre circulation des données à caractère personnel entre Etats membres ». Mais cette liberté de circulation reposait sur le consentement de l'individu, dont le recueil était prévu par l'article 7 de la directive. Celui-ci indiquait qu'un traitement de données ne pouvait être effectué, entre autres, que si la personne concernée avait « indubitablement donné son consentement ». La place du consentement dans le dispositif protecteur est devenue primordiale : il permettait non seulement de légitimer le traitement de données réalisé, mais il était également à l'origine de l'obligation d'information pesant sur les responsables de traitement. Par ailleurs, le texte de la directive a permis, en théorie, une uniformisation des règles protectrices. Celle-ci est passée par l'adoption de définitions unifiées permettant de déterminer avec certitude les hypothèses dans lesquelles les opérations devaient être encadrées par les règles de la directive.

b. La construction progressive d'un droit fondamental

49. Le développement des technologies de la communication constitue une liberté nouvelle, celle d'échanger et de recevoir des informations en quantité toujours

plus importante. Mais elle est aussi une source potentielle d'atteinte aux droits existants que les objets connectés et le *quantified-self* contribuent à entretenir.

Les Etats ont, par le truchement du Conseil de l'Europe et de l'Union européenne, progressivement érigé le droit à la protection des données à caractère personnel au rang des droits fondamentaux reconnus à l'individu. La notion de droit fondamental est susceptible de faire l'objet de plusieurs acceptions mais le droit à la protection des données semble s'être imposé comme devant faire l'objet d'un nombre limité de restrictions de la part des Etats. Le processus de construction de ce droit révèle son autonomisation au regard de l'évolution des technologies de l'information et de la communication. Auparavant apprécié à l'aune du droit fondamental au respect de la vie privée, celui-ci s'est progressivement différencié pour être doté d'un fondement juridique propre.

50. Un droit fondamental rattaché à la protection de la vie privée – L'adoption de la directive 95/46/CE marqua le point de départ de la construction progressive d'un droit communautaire de la protection des individus face aux traitements automatisés de données à caractère personnel. L'harmonisation des différentes législations nationales opérée par ce texte a semblé être un terreau fertile permettant la consécration d'un droit fondamental à la protection des données à caractère personnel. Associée à l'internationalisation des transferts de données, cette consécration est apparue nécessaire au regard des risques que le recours croissant au numérique par les administrations et les entreprises privés font potentiellement courir aux individus.

L'Union européenne, au départ réticente, a finalement contribué à la reconnaissance du caractère fondamental d'un tel droit[137], ensuite importé par la France « depuis des pays ou le développement de l'Etat de droit et la promotion des

[136] *Ibid*., considérant 3.
[137] Voir notamment : Emilie Debaets, *Le droit à la protection des données personnelles, Recherche sur un droit fondamental*, Thèse pour obtenir le grade de docteur de l'Université Paris 1 Panthéon-Sorbonne, présentée et soutenue publiquement le 12 décembre 2014, p. 12.

droits des individus ont opéré par voie essentiellement juridictionnelle »[138]. Comme le souligne Stéphanie Hennette-Vauchez, la notion de droit fondamental n'est pas univoque : elle est susceptible de renvoyer à l'idée d'importance de la norme dégagée, mais aussi signifier qu'une norme est le fondement d'autres droits. En outre, « la notion de fondamentalité des droits aurait à voir avec leur capacité à prévaloir à la fois substantiellement sur d'autres droits et, le cas échéant, sur des normes juridiques »[139].

Par ailleurs, étant donné que « les droits de l'homme et les libertés fondamentales ne sont pas seulement un état du droit à un moment donné, mais constituent aussi des objectifs à atteindre dans une société, dans les Etats ou dans le monde »[140], cette consécration a semblé pertinente au regard du caractère éminemment évolutif des technologies utilisées pour procéder à des collectes de données à caractère personnel. L'impossibilité de pouvoir prévoir avec certitude l'évolution des technologies et les nouvelles modalités de collecte et de traitement de données à caractère personnel pouvait en effet justifier d'ériger le droit à la protection des données au rang de droit fondamental afin que celui-ci irrigue en permanence l'ensemble des dispositions protectrices.

51. Cette construction d'un droit fondamental européen à la protection des données à caractère personnel s'est opérée de manière progressive par la mobilisation de différents instruments juridiques européens. Un premier fondement juridique particulier a pu être mobilisé pour parvenir à cette consécration, confirmant par ailleurs le lien existant entre le droit au respect de la vie privée et la protection des données à caractère personnel. Ainsi, le droit fondamental à la protection des données a d'abord pu être caractérisé par son rapprochement au droit au respect de la vie privée et familiale.

La Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, Traité international signé par les Etats membres du Conseil de l'Europe le 4 novembre 1950 et entré en vigueur le 3 septembre 1953 consacre, en

[138] Stéphanie Hennette-Vauchez, Diane Roman, *Droits de l'Homme et libertés fondamentales*, Dalloz, HyperCours, 1ère édition, 2013, p. 12.
[139] *Ibid.*, p. 13.

son article 8, le fait que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ». Cette convention ne consacre pas spécifiquement de droit à la protection des données à caractère personnel mais la Cour européenne des droits de l'homme s'est fondée sur l'article 8 pour faire de ce droit une composante du droit au respect de la vie privée. Elle a notamment mobilisé les principes de la Convention n° 108 pour l'interprétation de cet article 8 de la CESDH et plusieurs décisions, *Amann*[141], *Rotaru*[142] ou *Khelili*[143], ont montré ces liens. Selon une jurisprudence désormais constante, la Cour indique que « la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit à la vie privée et familiale consacré par l'article 8 de la Convention »[144]. Ce droit fondamental à la protection des données à caractère personnel a par la suite été consacré de façon autonome.

52. Un droit fondamental autonome – L'Union européenne a également fait de la protection des données à caractère personnel un droit fondamental. Dès 1975, le Parlement européen exprimait la nécessité de doter l'Union future d'une Charte des droits fondamentaux[145]. Après plusieurs travaux[146] témoignant de la volonté de « renforcer le statut des droits fondamentaux dans le projet d'intégration européenne »[147], la Charte des droits fondamentaux de l'Union européenne fut proclamée une première fois à Nice le 7 décembre 2000.

Officiellement adoptée dans sa version définitive par les présidents de la Commission européenne, du Parlement et du Conseil de l'UE le 12 décembre 2007, la Charte consacre dans un article 8 le droit, pour toute personne, à la protection des données à caractère personnel la concernant. S'inspirant des dispositions de la directive de 1995, cette Charte mentionne, outre le droit à la protection des données à

---

[140] Henri Oberdorff, *Droits de l'Homme et libertés fondamentales*, LGDJ Lextenso Editions, 5ème édition, 2015, p. 23.
[141] CEDH, 16 février 2000, *Amann c. Suisse*, n° 27798/95.
[142] CEDH, 4 mai 2000, *Rotaru c. Roumanie*, n° 28341/95.
[143] CEDH, 18 octobre 2011, *Khelili c. Suisse*, n° 16188/07.
[144] CEDH, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, requêtes n° 30562/04 et 30566/04.
[145] JO C 179 du 6 août 1975, p. 28.
[146] Résolution du Parlement européen du 2 avril 1989 sur la déclaration des droits et libertés fondamentales, JO C 120, 6 mai 1989, p. 51.
[147] Nicolas Cariat, *La Charte des droits fondamentaux et l'équilibre constitutionnel entre l'Union européenne et les Etats membres*, Collection du Centre des droits de l'homme de l'Université catholique de Louvain, Bruylant, 2016, p. 150.

caractère personnel, les principes clés relatifs à cette protection[148], ainsi que la garantie du contrôle de la mise en œuvre de ces principes par une autorité indépendante[149]. Ainsi, alors que l'on a longtemps déploré l'absence de droits fondamentaux directement issus des traités européens[150], le droit à la protection des données est désormais un droit fondamental qui relève du droit dérivé de l'Union. C'est un droit qui dispose d'une dualité de fondements juridiques, le protocole n°14 à la CEDH ayant effectivement ouvert à l'Union européenne la possibilité de devenir partie à la Convention, possibilité concrétisée par l'article 6, 2) du traité de Lisbonne.

3. Un mouvement législatif européen renouvelé

53. La directive de 1995, transposée en France en 2004, est un texte qui a permis, en raison du principe de neutralité technologique mis en œuvre, de prendre en compte et de s'adapter au développement de nouvelles technologies. Pourtant, l'adoption de cette directive a eu lieu bien avant la démocratisation d'instruments qui ont profondément modifié le rapport aux données à caractère personnel des individus : moteur de recherche en ligne et messagerie (*Google*), commerce en ligne (*Amazon*), réseaux sociaux permettant aux individus de révéler des éléments relatifs à leur vie privée (*Facebook*) ou encore smartphones permettant la mobilité de tous ces précédents services (*Apple*).

La généralisation des services proposés par les GAFAM a représenté un enjeu important pour le cadre juridique en vigueur. Généralisation des transferts internationaux de données, traitement à grande échelle, géolocalisation, publicité ciblée, partage de contenu, mobilité des services, instantanéité de la collecte : ces éléments n'avaient pas été pris en compte par les rédacteurs de la directive[151]. La généralité des termes employés par le texte a permis l'encadrement de ces nouveaux

[148] L'article 8, 2 de la Charte dispose que « les données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification ».
[149] L'article 8, 3 de la Charte dispose que « le respect de ces règles est soumis au contrôle d'une autorité indépendante ».
[150] Bertrand Favreau, « La protection des données à caractère personnel », *IDHAE*, 2009, p. 7.
[151] Le Règlement (UE) 2016/679 du 27 avril 2016 prend acte, dans le considérant 6, de ces évolutions et indique notamment : « L'ampleur de la collecte et du partage de données à caractère personnel a augmenté de manière importante. Les technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités. De plus en plus, les personnes physiques rendent des informations les concernant accessibles publiquement et à un niveau mondial ».

procédés mais un point particulier a fait défaut avec l'avènement de ces nouveaux moyens de collecte : les modalités de contrôle, par les individus, de l'utilisation faite de leurs données par des tiers.

54. Un contexte particulier – L'augmentation du nombre de services en ligne reposant sur l'économie de la donnée a justifié qu'un texte nouveau soit adopté, afin de responsabiliser les entreprises du numérique. Le contexte particulier dans lequel le Règlement général européen a été adopté a confirmé la nécessité de réformer le dispositif en vigueur. La survenance d'un certain nombre d'événements a en effet mis en lumière les limites de la réglementation tout en permettant de rendre le sujet de la protection des données à caractère personnel visible dans le débat public.

D'abord, l'arrêt dit *Google Spain* de la CJUE en date du 13 mai 2014 a posé la question du droit au déréférencement. La Cour a indiqué que l'exploitant d'un moteur de recherche était obligé de supprimer de la liste de résultats les liens concernant un individu lorsque ces informations n'étant plus pertinentes au regard du temps écoulé[152]. Le texte définitif du Règlement a repris à son compte cette possibilité[153].

Une seconde affaire, en date du 6 octobre 2015, a montré les limites relatives aux transferts de données entre l'Europe et les Etats-Unis[154]. L'accord dit *Safe Harbor* visant à réglementer ces transferts et à attester du niveau de protection équivalent outre-Atlantique a ainsi été annulé par la Cour, en raison du manque de protection suffisante accordée. Un nouvel accord intitulé *Privacy Shield* est par la suite intervenu entre l'Europe et les Etats-Unis et le Règlement général européen est venu renforcer les règles relatives aux transferts internationaux de données[155]. Ces deux affaires, dont la Cour de justice de l'Union a eu à connaître, s'inscrivent dans un

---

[152] CJUE, gr. ch., 13 mai 2014, *Google Spain SL, Google Inc. c. Agencia Espanola de la Proteccion de Datos et Mario Costeja Gonzalez*, aff. C-131/12 ; *AJDA* 2014. 1147, chron. M. Aubert, E. Broussy et H. Cassagnabère ; D. 2014. 1476, note V.-L. Benabou et J. Rochfeld ; *ibid*. 1481, note N. Martial-Braz et J. Rochfeld ; *ibid*. 2317, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; *AJCT* 2014. 502, obs. O. Tambou ; *Constitutions* 2014. 218, chron. D. de Bellescize ; *RTD eur*. 2014. 283, édito. J.-P. Jacqué ; *ibid*. 879, étude B. Hardy ; *ibid.* 2016. 249, étude O. Tambou ; Rev. UE 2016. 597, étude R. Perray.
[153] Cf., *infra*, n° 324.
[154] CJUE, gr. ch., 6 octobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, aff. C-362/14 ; D. 2016. 111, note B. Haftel, 88, point de vue C. Castets-Renard, et 2025, obs. S. Bollée ; *AJDA* 2015. 2257, chron. E. Broussy, H. Cassagnabère et C. Gänser ; *AJ pénal* 2015. 601, obs. E. Daoud ; *Dalloz IP/IT* 2016. 26, étude C. Théard-Jallu, J.-M. Job et S. Mintz ; *JAC* 2015, n° 29, p. 11, obs. E. Scaramozzino ; JT 2015, n° 180, p. 14, obs. E. Scaramozzino ; *RTD eur*. 2015. 786, obs. M. Benlolo-Carabot, 2017. 361 et 365, obs. F. Benoît-Rohmer.
[155] Céline Castets-Renard, « L'adoption du *Privacy Shield* sur le transfert de données personnelles », *Rec. Dalloz*., 2016, p. 1696.

contexte plus vaste de prise de conscience, par les individus, des problématiques relatives au fichage et à la surveillance de masse.

55. Les révélations d'Edward Snowden en 2013 concernaient principalement l'enregistrement indifférencié par la NSA de métadonnées, traces numériques créées lors de l'utilisation de services connectés. Mais la participation à cette surveillance des géants du numérique tels que Google ou Apple a été soulevée, en raison notamment du programme *PRISM* qui permettait à la NSA d'avoir accès aux serveurs de certaines de ces compagnies. Plus récemment, c'est le réseau social Facebook qui était en 2016 au cœur d'une polémique, à la suite des révélations de l'affaire dite *Cambridge Analytica*. Notamment utilisé par l'actuel président américain lors de sa campagne, cette société britannique aurait eu accès aux données de 30 à 70 millions d'utilisateurs à l'aide d'un quizz proposé sur le réseau social. Cet évènement, largement commenté[156], a notamment conduit à l'audition de Mark Zuckerberg, fondateur de Facebook, devant le Sénat américain et le Parlement européen[157].

Ces différents éléments, qu'il s'agisse des décisions de la CJUE ou des révélations opérées, présentent un certain nombre de problématiques : transferts internationaux de données, partage d'informations sur les réseaux sociaux ou encore, création de métadonnées par l'utilisation de services. Or, le *quantified-self*, par son mode de fonctionnement, a pour particularité de cumuler ces différents aspects et donc, les diverses problématiques qui y sont liés. La survenance de ces évènements et leur couverture médiatique en pleine procédure d'adoption du Règlement général ont permis une prise de conscience des problématiques liées à la protection des données tout en confirmant la nécessité de renouveler le cadre juridique.

56. L'élaboration du RGPD – Le Règlement général européen adopté en 2016 insiste sur la problématique relative aux capacités de maîtrise des informations en indiquant, au considérant 7, que « les personnes physiques devraient avoir le

[156] Voir notamment : Philippe Mouron, « De la rumeur aux fausses informations », *Légicom*, 2018, p. 53 ; Faustine Jacomino, « Mise en conformité des conditions générales d'utilisation de Facebook : la Commission européenne s'impatiente », *AJ Contrat*, 2018, p. 521 ; Pierre Sirinelli, Stéphane Prévost, « To be or Notes to be ? », *Dalloz IP/IT*, 2018, p. 205 ; Emilie Seruga-Cau, Tiphaine Havel, « Campagne électorale et utilisation des données personnelles : grands principes et points de vigilance », *AJCT*, 2019, p. 73 ; Alexis Déroudille, Farid Fatah, « L'extraterritorialité du RGPD dans le contexte du « Cloud Act » », *Rev. UE*, 2019, p. 442.
[157] Guerric Poncet, « L'audition tendue de Marc Zuckerberg au Parlement européen », *Le Point*, 23 mai 2018.

contrôle des données à caractère personnel les concernant ». Cette affirmation est au cœur du renouveau du cadre juridique protecteur dont le RGPD est à l'origine. Dès 2012 a été envisagé le remplacement de la directive de 1995[158], les divergences entre Etats membres dans la transposition de celle-ci menant à une fragmentation de la protection des données en Europe et constituant donc un frein à la croissance économique et à l'innovation. Quatre années seront nécessaires pour procéder à la réforme du cadre européen de protection des données personnelles[159], la version définitive du texte ayant été publiée le 4 mai 2016 au Journal officiel de l'Union européenne.

Différentes raisons permettent d'expliquer qu'un tel délai ait été nécessaire afin de trouver un consensus sur le texte préparé. D'abord, le recours à un règlement plutôt qu'à une directive a laissé, de fait, moins de marge de manœuvre aux Etats pour que ceux-ci puissent adapter leur cadre juridique national. Il a donc été nécessaire de trouver, en amont, un véritable consensus entre tous les Etats membres afin que ceux-ci acceptent finalement d'adopter le texte. Ensuite, ce sont des problématiques d'ordre économique qui ont fait l'objet d'âpres négociations entre les géants du numérique et les instances européennes. Le nouveau cadre juridique proposé, pour permettre aux individus de mieux contrôler l'utilisation qui est faite de leurs données, renouvelle les obligations pesant sur les responsables de traitement. Le meilleur encadrement des transferts internationaux de données prévu par le texte s'accompagne ainsi de sanctions renforcées pour les opérateurs du numérique. Celles-ci peuvent en effet atteindre, selon l'article 83 du texte, un montant allant jusqu'à vingt millions d'euros ou quatre pour cent du chiffre d'affaires annuel mondial. Un important travail de *lobbying* a donc été réalisé en amont par les grandes entreprises du numérique afin de faire valoir leurs intérêts et tenter d'abaisser le montant des sanctions encourues. Plusieurs documents consignent les rencontres entre les membres de la Commission et des représentants des firmes du numérique[160]. Par ailleurs, un documentaire intitulé *Democracy* réalisé par David Bernet et sorti en

[158] « The EU Data Protection Reform 2012 : Making Europe the Standard Setter for Modern Data protection rules in the digital age », *Innovation Conference Digital, Life, Design*, Munich, 22 January 2012 (discours).
[159] Proposition de Règlement du Parlement européen et du Conseil 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, 25 janvier 2012.
[160] Voir notamment : https://www.integritywatch.eu/

2015, montre bien les négociations que Jan Philipp Albrecht, rapporteur du projet de Règlement, a dû mener avec les géants du numérique[161].

57. Entre continuité et rupture – Le Règlement général européen s'inscrit dans la continuité des acquis de la directive de 1995. Les principes essentiels à la mise en œuvre d'opérations de traitement de données sont conservés, qu'il s'agisse du principe de finalité nécessitant que les données soient traitées dans un but déterminé à l'avance, du principe de proportionnalité de la collecte à la finalité ou encore du principe de durée limitée de conservation des informations traitées. Le consentement de l'individu est toujours nécessaire pour mettre en œuvre un traitement de données et la personne en charge de traiter des données doit délivrer une information détaillée quant aux raisons et modalités de la collecte. Au cœur du dispositif protecteur avant l'adoption du nouveau texte européen, ces principes ont été repris et parfois précisés : le consentement doit être donné sous une forme particulière et l'information délivrée doit être plus aisément compréhensible. Un important travail à également été réalisé afin de compléter les définitions déjà présentées dans l'ancien texte : données à caractère personnel, données sensibles, responsable de traitement, sous-traitant ou encore et entre autres, traitement transfrontalier. Le principe de neutralité technologique, sous-jacent dans le cadre de la directive de 1995, est confirmé par le Règlement européen et désormais explicitement mentionné[162]. Ce principe suppose l'applicabilité des règles protectrices à tous les traitements de données à caractère personnel réalisés, indépendamment du moyen mis en œuvre pour y parvenir. Il permet donc la prise en compte de l'automesure connectée par la réglementation.

58. Mais, si le RGPD reprend certains éléments préexistants, il opère aussi une véritable révolution avec l'abandon quasi-systématique des formalités préalables à la mise en œuvre d'un traitement de données. Il faut reconnaître que la multiplication des traitements, leur automatisation ainsi que leur permanence avaient rendu inefficace le système de déclaration préalable des traitements auprès d'autorités administratives indépendantes. D'abord, un certain nombre de dispenses et normes simplifiées avaient été mises en place par la CNIL pour les traitements les plus

[161] David Bernet, *Democracy, la ruée vers les datas*, 2015.

courants de données à caractère personnel. Ensuite, le nombre exponentiel de traitements de données mis en œuvre a nui à la pertinence de cette procédure. En effet, l'objectif de ce régime déclaratif préalable était de permettre la vérification, avant même la mise en œuvre du traitement, de la conformité de celui-ci aux règles protectrices des données à caractère personnel. Ce système a pourtant montré d'évidentes limites. Les objets connectés, en automatisant la mise en œuvre de traitements tout en augmentant considérablement leurs nombres, ont nui à l'objectif de traçabilité associé aux formalités préalables. Surtout, ils ont compliqué la faculté, pour les autorités administratives indépendantes, de procéder à des contrôles *a posteriori* efficaces. Les capacités concrètes d'action de ces autorités ont donc été réduites par l'accroissement du nombre de responsables de traitement, mais également par la diversité de ces mêmes traitements.

Sur fond de simplification, le RGPD a supprimé de nombreuses formalités préalables auprès de la CNIL. En contrepartie, les structures doivent assurer une protection renforcée des données à chaque instant et surtout être en mesure de la démontrer en documentant leur conformité. Ce changement démontre qu'il règne dans l'esprit du règlement « une responsabilisation plus qu'une responsabilité »[163] des acteurs. Le changement de paradigme opéré par le règlement implique donc pour les opérateurs de « vérifier au coup par coup si chaque utilisation des données est conforme aux droits des personnes concernées et à la réglementation »[164]. Un principe dit d'*accountability* ou de conformité a donc remplacé ce système et doit permettre à chaque responsable de traitement de démontrer qu'il traite des données à caractère personnel de façon conforme à la réglementation. Ce principe est non seulement sensé permettre une meilleure traçabilité des opérations réalisées mais il doit également garantir aux individus que leurs droits sont mieux respectés, conformément au principe d'autodétermination informationnelle.

---

[162] Le considérant 15 mentionne ainsi que pour éviter « de créer un risque grave de contournement, la protection des personnes physiques devrait être neutre sur le plan technologique et ne devrait pas dépendre des techniques utilisées ».
[163] Sonia Zouag, « A grands pouvoirs, grandes responsabilités », *JT*, 2018, n° 204, p. 3.
[164] François Viney, « La loi relative à la protection des données personnelles », *AJ Famille*, 2018, p. 366.

59. L'autodétermination informationnelle. Initialement dégagée par la Cour constitutionnelle fédérale allemande en 1983, l'autodétermination doit permettre à l'individu de maîtriser et de contrôler l'usage qui est fait de ses données à caractère personnel. La loi Informatique et Libertés, modifiée en juin 2018 pour prendre en compte les évolutions du règlement, y fait explicitement référence dans son article 1er, alinéa 2, indiquant que « toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel ». Désormais réécrite[165], la loi Informatique et Libertés consacre toujours cette idée de contrôle de l'utilisation des données des individus. Les autorités administratives indépendante, en dehors de leurs pouvoirs de sanction renforcés, vérifient également que cette autodétermination est effective et aident les responsables de traitement dans la mise en œuvre de leur obligation de conformité.

60. Un champ d'application élargi – La règlementation relative à la protection des données à caractère personnel doit, pour être efficace, couvrir un nombre important de situations.

1) *Rationae materiae*. Le champ d'application élargi du RGPD permet au cadre juridique de rester pertinent face aux évolutions et aux mutations des technologies, notamment à l'œuvre avec l'automesure connectée. Celle-ci implique de nombreux acteurs et les traitements réalisés sont de nature variée. Le principe de neutralité technologique permet de garantir la pérennité de la réglementation mais son champ d'application a dû être précisé par le Règlement européen. En effet, outre des modalités de collecte et de traitement renouvelées, le *quantified-self* présente des spécificités relatives au nombre de personnes appelées à intervenir dans la chaîne de traitement, ainsi qu'à leur localisation géographique.

2) *Rationae personae*. L'élargissement du champ d'application des règles protectrices doit permettre de conférer aux individus une plus grande visibilité des informations traitées à leur égard. Le RGPD procède ainsi à une meilleure répartition des responsabilités des personnes appelées à traiter des données tout en permettant une meilleure identification de ces personnes. Ce champ d'application révisé doit

[165] Ordonnance n°2018-1125 du 12 décembre 2018.

aussi permettre une meilleure adaptabilité du cadre juridique aux spécificités propres aux traitements réalisés par le biais d'objets connectés. Vitesse, automatisation, permanence ou encore diversité des mesures sont susceptibles de complexifier l'identification précise des différents opérateurs, notamment lorsque ceux-ci sont géographiquement dispersés.

3) *Rationae loci*. Le numérique a pour particularité de se jouer des frontières terrestres. L'apparition d'Internet a permis l'affranchissement progressif de ces frontières au profit d'un espace virtuel globalisé favorisant le partage d'informations entre individus. Les objets connectés, grâce à leur connexion à ce même réseau, s'inscrivent dans cet espace globalisé. Déjà en 1995, l'adoption de la directive a permis de procéder à un décloisonnement des droits nationaux au profit d'un mécanisme de confiance réciproque permettant le libre échange d'informations. Mais le climat de méfiance entourant les transferts outre-Atlantique de données[166] a justifié que le Règlement soit doté d'un champ d'application territorial élargi. Des critères alternatifs d'application sont instaurés. Ils s'inscrivent dans la droite ligne de la position de la Cour de justice qui avait déjà eu l'occasion de se prononcer en faveur d'une application territoriale large des règles de protection des données[167], application justifiée par le fait que le cyberespace est « par excellence le lieu de la déterritorialisation du droit »[168].

Le Règlement général procède ainsi à une rénovation du cadre juridique applicable aux traitements des données à caractère personnel et les évolutions proposées ont toutes vocation à s'appliquer aux spécificités du *quantified-self*. Pourtant, malgré ces transformations, le phénomène de l'automesure connectée vient profondément remettre en question les principes de protection réaffirmés tout en contribuant également au déplacement de la régulation.

---

[166] Une résolution du 5 juillet 2018, adoptée en séance plénière par les députés européens, appelait à la suspension du Privacy Shield, l'accord ayant été adopté par suite de l'invalidation du Safe Harbor par la Cour de justice de l'Union le 6 octobre 2015.

[167] CJUE, gr. ch., 13 mai 2014, *Google Spain SL, Google Inc. c. Agencia Espanola de la Proteccion de Datos et Mario Costeja Gonzalez*, aff. C-131/12.

[168] Jean-Philippe Foegle, « La CJUE, magicienne européenne du « droit à l'oubli » numérique », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 16 juin 2014, consulté le 03 août 2018.

B. Délimitation de la recherche et problématique

61. Formulation des hypothèses – La réforme d'ampleur proposée par le Règlement général européen, reprise par la dernière itération de la loi Informatique et Libertés de 2019, procède à un changement de paradigme du droit à la protection des données à caractère personnel. Le RGPD confère un rôle nouveau aux responsables de traitements, qui deviennent des acteurs à part entière de la protection des données à caractère personnel. Le rôle actif qui est donné aux opérateurs du numérique s'insère dans un mouvement plus général de contractualisation du droit à la protection des données[169] et justifie, à travers un certain nombre de mécanismes de conformité, le recours à la régulation tel qu'encouragé par le texte.

62. La question à laquelle nous devons répondre est celle de savoir si ce changement permet une prise en compte efficace des traitements d'automesure et si cette prise en compte instaure un niveau de protection satisfaisant des données à caractère personnel des individus. En effet, malgré le changement de paradigme évoqué, le RGPD repose à nouveau sur le principe de neutralité technologique, perçu comme l'absence de « discrimination entre tous types de technologie permettant de recevoir l'information »[170]. La question de savoir s'il ne faudrait pas dépasser le principe de neutralité technologique pour procéder à l'adoption d'un droit *ad hoc* doit également être soulevée. Nous nous demanderons ainsi, de façon incidente, si les nouveaux instruments de conformité utilisés ne permettent pas, *in fine*, de procéder à la création d'un droit spécifique pour chaque traitement. Dès lors, outre l'analyse de la réception des nouvelles technologies par le droit et de sa modification au contact du numérique, l'étude posera la question de l'efficacité des principes de protection instaurés par le RGPD.

63. Enjeux méthodologiques. L'étude de la pertinence des nouveaux principes instaurés par le RGPD entraîne, lorsqu'ils sont appliqués à la pratique de l'automesure connectée, un certain nombre de difficultés impliquant de délimiter précisément la recherche.

---

[169] David Larbre, « Données personnelles », *in* Bazex A., Eckert G, Lanneau R., Le Berre C., du Marais B., Sée A. (dir.), *Dictionnaire des régulations*, 2016, Lexis Nexis, p. 267.
[170] Karine Favro, *Droit de la régulation des communications numériques*, LGDJ, coll. Systèmes, 2018, p. 99.

64. Difficultés - Notre étude a tout d'abord été confrontée à la mutation quasi-permanente des objets techniques permettant de se livrer à la pratique de l'automesure connectée. A titre d'exemple, pas moins de six versions de la montre connectée d'Apple ont été proposés à la commercialisation depuis 2014, chacune des versions présentées proposant de nouvelles innovations technologiques intéressant directement notre étude. La commercialisation de ces dispositifs n'est pas sans conséquence. Disposant de nouveaux capteurs permettant d'affiner l'automesure, ils sont susceptibles de poser de nouvelles questions au regard des enjeux du sujet. De nombreuses applications d'automesure disponibles au téléchargement ont également été développées et mises à jour, leurs fonctionnalités étant à chaque fois améliorées, précisées et complétées.

Relayées par une importante littérature spécialisée, surtout outre-Atlantique[171], les évolutions technologiques s'accompagnent d'évolutions juridiques constantes. Si le texte du RGPD, principale source du droit de la protection des données personnelles, a été adopté définitivement en 2016, sa réception en droit français a été progressive et a nécessité l'adoption et la révision de multiples règles. Procédant d'abord par petites touches, en introduisant quelques dispositions dans la loi de modernisation de notre système de santé[172] et dans la loi pour une République numérique[173], le législateur a dû réviser en profondeur le cadre juridique de la protection des données pour adapter le droit français au droit de l'Union européenne : la réception du RGPD en droit français a nécessité l'adoption d'une loi, le 20 juin 2018[174], complétée en décembre de la même année par une ordonnance procédant à la réécriture du texte[175]. Enfin, une nouvelle loi relative à l'organisation et à la transformation du système de santé, susceptible d'impacter les dispositifs d'automesure, a été adoptée en juillet 2019[176].

---

[171] Voir par exemple : *Stanford Technology Law Review, Harvard Journal of Law & Technology, Harvard Business Review, Yale Journal of Law & Technology, MIT Technology Review, Wired, TechCrunch, Mashable, Computer World, Science Focus, Tech Advisor, International Journal of Law & Technology*.
[172] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.
[173] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.
[174] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.
[175] Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 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.
[176] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé.

65. Délimitation du terrain de recherche – Le sujet du droit de la protection des données à caractère personnel a déjà fait l'objet d'un certain nombre de travaux. Ceux-ci ont permis d'évoquer la place de ce droit au sein des droits fondamentaux[177], d'interroger son domaine d'application[178] ou encore de délimiter la portée de la protection qu'il met en oeuvre[179]. Notre étude fait le choix d'interroger la pertinence et les évolutions du cadre juridique relatif à la protection des données à travers le phénomène novateur de l'automesure connectée. En effet, cette pratique, qui n'a pas encore fait l'objet d'une étude d'ampleur, concentre aujourd'hui un nombre important de questionnements et de procédés qui sont généralement associés au droit de la protection des données à caractère personnel : qualification et volume des informations récoltées, recours à différents prestataires, services de *cloud computing* ou encore transferts internationaux de données. Ces éléments seront nécessairement convoqués pour étudier la mutation du droit au contact des nouvelles technologies employées pour la pratique de l'automesure connectée.

66. Le thème de l'automesure connectée, par la réunion de différentes problématiques, est un sujet au confluent de plusieurs disciplines. L'étude nécessite de mobiliser des éléments qui sont relatifs par exemple à l'informatique ou à la sociologie et qui permettent d'expliquer l'évolution des pratiques de l'automesure. Mais le sujet mobilise également différentes disciplines, relatives au droit privé et surtout au droit public.

Des éléments relatifs au droit privé et plus particulièrement au droit des biens seront étudiés. Les données traitées dans le cadre de l'automesure connectée contiennent, selon l'opinion majoritaire, des éléments relatifs à l'identité de la personne, insaisissables et inaliénables par nature[180]. Mais ces données doivent, selon d'autres[181], faire l'objet d'une patrimonialisation afin que les individus puissent profiter de la monétisation qui en est faite par les opérateurs du numérique. Cette

[177] Emilie Debaets, *Le droit à la protection des données personnelles, Recherche sur un droit fondamental, Thèse pour obtenir le grade de docteur de l'Université Paris 1 Panthéon-Sorbonne*, présentée et soutenue publiquement le 12 décembre 2014, 809 p.
[178] Sandie Alliot, *Essai de qualification de la notion de données à caractère personnel*, Thèse de doctorat en droit, présentée et soutenue publiquement le 15 janvier 2018, Université de Bourgogne Franche-Comté.
[179] Géraldine Criqui-Barthalais, *La protection des libertés individuelles sur le réseau Internet*, Thèse de doctorat en droit, présentée et soutenue publiquement le 7 décembre 2018, Université Paris-II Panthéon-Assas, 410 p.
[180] Conseil d'Etat, *Le Numérique et les droits fondamentaux*, Rapport Annuel, La Documentation Française, 2014, p. 267.
[181] Génération Libre, *Mes Data sont à moi. Pour une patrimonialité des données personnelles*, janvier 2018, p. 8.

conception n'a pas été retenue par le droit positif français, mais elle montre que des interrogations relatives à la qualification juridique des informations traitées sont soulevées. Ensuite, le recours à des sous-traitants dans le cadre de traitements de données ou la conclusion de contrats de fourniture de services en ligne impliquent de convoquer le droit des obligations. Enfin, des éléments de droit pénal sont également soulevés par l'étude, lorsque des manquements aux règles protectrices sont constatés.

Les aspects précédemment évoqués ne seront évidemment pas négligés, mais le choix est ici fait de voir le sujet sous l'angle des libertés fondamentales car il semble que le droit des données à caractère personnel est particulièrement impacté par l'émergence de la pratique de l'automesure.

Par ailleurs, sans procéder à une analyse comparée systématique, il en sera fait usage de manière ponctuelle, pour éclairer le raisonnement. L'étude s'appuiera en particulier sur une comparaison avec le droit applicable aux Etats-Unis, où le phénomène de l'automesure est né. L'analyse comparée avec ce système juridique sera d'autant plus précieuse que le droit qui s'y applique repose sur une conception différente de la conception européenne.

C. Annonce de plan

67. Pour vérifier l'hypothèse selon laquelle l'automesure connectée conduit à une remise en question des principes fondamentaux de la réglementation protectrice des données personnelles et ainsi à un déplacement de la régulation, l'étude impose de voir en premier lieu comment l'automesure connectée fragilise le cadre juridique existant pour voir en second lieu comment ce cadre juridique se reconstruit.

La première partie analyse les limites à l'appréhension de l'automesure par la réglementation : un travail de définition des données à caractère personnel sera réalisé, afin notamment d'identifier et de discerner les différentes catégories de données collectées lors de la pratique de l'automesure. Ce travail de définition, portant notamment sur la distinction entre donnée personnelle et donnée sensible, est essentiel pour rattacher l'automesure au cadre protecteur des données à caractère personnel. Il permet également de montrer en quoi le cadre juridique est fragilisé par

le développement de cette pratique et en quoi la réglementation actuelle présente certaines limites face à la démocratisation de ce phénomène technologique.

Le renouvellement du cadre juridique par le RGPD sera ensuite développé. L'étude du nouveau cadre juridique européen permettra de relever qu'un déplacement de la régulation, des Etats et autorités administratives indépendantes aux responsables de traitement et agences, est encouragé, conduisant à une profonde mutation du droit, dans son contenu mais aussi dans sa forme, le recours au droit souple étant privilégié.

Partie 1 : La fragilisation du cadre juridique

Partie 2 : La reconstruction du cadre juridique

PREMIÈRE PARTIE – LA FRAGILISATION DU CADRE JURIDIQUE

68. Le *quantified-self* ou automesure connectée se présente sous la forme d'un véritable écosystème : il repose sur l'utilisation et la mise en relation d'outils numériques de natures variées qui communiquent entre eux. Il n'existe, dès lors, pas un *quantified-self* unique et standardisé, mais différentes formes d'automesures connectées reposant chacune sur la corrélation de différents instruments, au gré des besoins des utilisateurs. Objets connectés, applications mobiles, *smartphones*, tablettes ou encore réseaux sociaux sont autant d'éléments qui composent cet écosystème et qui sont capables d'aider l'individu à obtenir des informations sur ses habitudes de vie, son bien-être ou encore sa santé. Ces éléments sont ensuite mis en relation par la connexion à Internet des différents médias proposés. Cette connexion permet de préciser les informations délivrées aux individus dans le cadre de l'automesure mais également de les analyser, de les stocker ou de les conserver. Dans certains cas, une comparaison des informations collectées avec celles d'autres personnes est rendue possible, renforçant l'idée qu'il existe une communauté d'utilisateurs pratiquant l'automesure.

Les données collectées, représentation matérielle des informations relevées par les différents instruments de mesure, sont susceptibles d'être hautement identifiantes puisqu'elles visent directement l'intimité de l'individu. Relatives entre autres à l'activité physique, ces informations sont, de manière plus générale, en rapport direct avec le bien-être de l'individu. Par ailleurs, la routinisation des processus mis en œuvre, nécessaire pour établir des constantes sur lesquelles les individus pourront s'appuyer pour modifier leurs comportements ou suivre certaines évolutions, renforce la précision et la singularité des données collectées. L'interconnexion de ces dernières, rendue possible par des capacités de croisement renforcées par les progrès technologiques, est également à même d'apporter un degré de précision supplémentaire aux informations collectées. Ces différents éléments sont dès lors

susceptibles de questionner la pertinence du cadre juridique protégeant actuellement de telles données.

69. L'enjeu du sujet consiste d'abord à pouvoir déterminer avec précision quelle est la qualification juridique à apporter aux opérations réalisées et aux informations traitées. En effet, les nouveautés technologiques utilisées par le *quantified-self* complexifient la détermination du régime juridique protecteur applicable. Différentes chaînes de traitement de données sont exécutées et la connexion à Internet des objets utilisés afin de faciliter l'automatisation de la transmission d'informations sont des phénomènes relativement nouveaux. Une décomposition de chacune des opérations réalisées, entre collecte, traitement, analyse, stockage et transfert, est nécessaire afin de qualifier juridiquement cette pratique : les différents aspects de l'automesure doivent dès lors s'effacer pour laisser place à une identification précise des éléments mis en œuvre.

Cette décomposition des différentes opérations permet de rattacher la pratique de l'automesure à la réglementation relative à la protection des données à caractère personnel. La nature des informations collectées et l'étendue des moyens employés pour procéder à leur recueil ainsi qu'à leur analyse sont autant d'éléments qui conduisent à mobiliser le régime juridique contenu en France au sein de la loi Informatique et Libertés et au sein du RGPD au niveau européen. Fondé sur une exposition constante de soi et d'éléments relevant de la vie privée et de l'intimité corporelle d'une personne[182], la pratique de l'automesure s'alimente d'éléments relatifs à la vie privée qui sont directement relevés par les capteurs inclus dans les objets connectés et autres supports utilisés. La divulgation de données à caractère personnel, traduction de la notion de vie privée lorsqu'elle est appliquée au domaine du numérique[183], devient dès lors une condition nécessaire à l'existence des services eux-mêmes. Les différents textes en vigueur, malgré leurs termes relativement généraux, ne font pas mention des objets connectés. Ces derniers posent pourtant des défis imprévus en matière de protection de la vie privée.

[182] Deborah Lupton, « Quantifying the body : monitoring and measuring health in the age of mHealth technologies », *Critical Public Health*, 2013, n°23, p. 393 à 403.
[183] Adrien Jammet, *La prise en compte de la vie privée dans l'innovation technologique*, Thèse pour obtenir le grade de docteur en droit, Université Lille 2, 14 février 2018, 397 p.

70. Le cadre juridique protecteur des données à caractère personnel a fait l'objet d'une première réforme d'ampleur en 1995, avec l'adoption de la directive 95/46/CE qui a permis la modification de la LIL en 2004. Celle-ci a été suivie par l'adoption du RGPD le 27 avril 2016 afin de permettre son adaptation à des capacités renouvelées de collecte, de traitement et de croisement de données. Une loi du 20 juin 2018 relative à la protection des données a par ailleurs été adoptée afin d'adapter la loi Informatique et Libertés de 1978 aux nouvelles dispositions du règlement[184] et de la directive « police-justice »[185] et une ordonnance du 12 décembre de la même année est venue procéder à la réécriture de la loi[186]. Ces dispositions protectrices ne mentionnent pas explicitement le *quantified-self,* mais celles-ci ont en principe vocation à mieux appréhender le changement de paradigme induit par les objets connectés, fondé sur une révélation volontaire de la vie privée et sur une expertise fondée sur l'exposition de soi. La prise en compte de ce changement de paradigme a été rendu nécessaire par le fait que des entreprises proposent aujourd'hui des outils numériques ayant pour but de collecter un nombre toujours plus important de données afin de proposer des services personnalisés.

Miniaturisation et accessibilité des outils utilisés permettent un accroissement effectif du flot d'informations disponibles, susceptible d'impacter la vie privée des individus dans la mesure où les données correspondent à des données personnelles, « reflet moderne de la personnalité »[187]. Le *quantified-self*, en tant qu'émanation de l'Internet des objets, pose de nouvelles questions relatives à la protection à apporter à l'utilisateur, étant donné que celui-ci est directement producteur de données via son corps et son activité physique et ce afin de déterminer son niveau de bien-être. Le droit à la protection des données à caractère personnel, malgré son évolution, est soumis à des défis qui restent relativement nouveaux, entre capacités de collecte

[184] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.
[185] Directive (UE) 2016/680 du Parlement européen et du Conseil, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.
[186] Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 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.
[187] Vincent Mazeaud, « La constitutionnalisation du droit au respect de la vie privée », *Les Nouveaux Cahiers du Conseil constitutionnel*, n° 48, 2015, p. 9.

multipliées, moyens de traitement automatisés ou encore diversité des mesures réalisées. La pratique de l'automesure nécessite donc, pour sa mise en œuvre, l'accomplissement de nombreuses opérations portant sur des données qui sont de nature variée. Celles-ci peuvent dès lors être difficiles à identifier **(Titre I)**, limitant ainsi la protection qui doit leur être apportée **(Titre II)**.

TITRE I – L'IDENTIFICATION COMPLEXE DE L'AUTOMESURE CONNECTÉE

71. La question de l'appréhension du *quantified-self* par la réglementation nécessite d'abord d'envisager et d'interroger la nature des données qui sont collectées dans ce cadre. En effet, les objets utilisés pour recueillir et traiter les données des individus sont relativement nouveaux et les données collectées apparaissent ainsi comme le support d'un éventuel risque informationnel pour l'individu. Perçu concrètement comme le risque de perte de maîtrise par celui-ci d'informations le concernant, ce risque semble déjà encadré par des règles existantes qui identifient la nature des données en question. Pourtant, le prisme de l'objet connecté ou des autres médias s'inscrivant dans le domaine de l'automesure pose la question de savoir si l'on assiste à la création d'un nouveau type de donnée, spécifique au *quantified-self*. Les données collectées dans ce cadre sont par nature variées : relatives à la condition physique, au sommeil, à l'alimentation ou encore à certains éléments relatifs à la santé, elles s'inscrivent de manière plus générale dans le cadre des éléments relatifs au bien-être.

Cette notion de bien-être ne fait pourtant l'objet d'aucune définition juridique précise à l'heure actuelle. Elle n'est pas reconnue au titre des éléments de réglementation relatifs à la protection des données personnelles et ne fait l'objet d'aucune mention par les différents textes concernés. Rien ne s'oppose pourtant à ce que ceux-ci s'appliquent aux données relatives au bien-être de l'individu. Fondés à l'origine sur la référence à la notion d'information nominative, les textes distinguent d'une part, les données à caractère personnel au sens classique du terme et d'autre part, les données dites sensibles et nécessitant une protection renforcée. Ces deux catégories ne donnent pas d'indications précises quant à leur contenu mais semblent directement applicables aux données issues du *quantified-self*. Les données collectées et traitées, traduction matérielle d'informations relatives à la vie privée et au domaine

de l'intime, ont ainsi vocation à être protégées par la réglementation relative à la protection des données personnelles.

72. Outre le renouvellement des modalités de collecte des informations et un changement d'approche fondé sur une révélation encouragée de l'intime, les données collectées ne présentent en apparence pas de spécificités particulières. Celles-ci, perçues sous l'angle de deux qualifications juridiques distinctes, simples données à caractère personnel ou données sensibles relatives dans certains cas à la santé, devraient dès lors avoir vocation à être protégées par la réglementation et par les différents textes qui la composent. Pourtant, les capacités de collecte, de croisement ou de transfert des données relevées questionnent la pertinence de leur rattachement à l'une ou l'autre des catégories mentionnées et l'automesure, par la mise en relation d'informations, soulève un doute quant à la qualification juridique précise à apporter aux données traitées. Bien que théoriquement identifiées juridiquement **(chapitre 1)**, les données d'automesure font l'objet d'une classification juridique incertaine **(chapitre 2)**.

CHAPITRE I – LA QUALIFICATION DES INFORMATIONS ISSUES DE L'AUTOMESURE CONNECTÉE

73. L'automesure s'est entièrement automatisée avec le développement du numérique et en particulier avec celui des objets connectés qui permettent un recueil continu de données. Ces dernières peuvent également être collectées par une application mobile destinée à un *smartphone* ou une tablette et elles ont pour particularité de toucher à l'intimité, voire à la santé. L'étude des enjeux juridiques de l'automesure connectée doit donc mener, en premier lieu, à étudier la nature des données qui sont traitées dans ce cadre par les différents instruments utilisés[188].

La numérisation de l'activité humaine étant rendue possible par l'utilisation de capteurs, l'enjeu est dès lors de savoir si les données en question ne sont pas tributaires de l'objet ou du média ayant permis leur collecte[189]. Les constantes de l'individu étant ainsi directement relevées, la question se pose également de savoir si les données traitées viennent s'intégrer au sein de catégories juridiques existantes et identifiées. Or, parmi ces catégories juridiques, celles contenues au sein de la loi Informatique et Libertés de 1978 modifiée et réécrite semblent les plus à même d'apporter une réponse à cette question. L'utilisation du numérique permet en effet de se référer aux principes déjà dégagés par ce texte tout en affirmant que les données en question ne sont pas tributaires de l'objet ou du média ayant permis leur collecte.

74. Les données collectées, identifiées par la réglementation en vigueur, sont donc intégrées au sein des catégories de données existantes et établies par la loi. Celles-ci perdurent en effet depuis leur instauration pour permettre aujourd'hui la prise en compte des données traitées dans le cadre de l'automesure, préalable nécessaire à l'application d'un régime juridique protecteur. L'objectif de cette loi, que ce soit dans sa rédaction initiale ou dans les modifications reçues d'abord par la

[188] Alain Rallet, Fabrice Rochelandet, « Exposition de soi et décloisonnement des espaces privés : les frontières de la vie privée à l'heure du numérique », *Terminal*, n° 105, 2010, p. 71 à 86.
[189] CNIL, « Le Quantified self : nouvelle forme de partage des données personnelles, nouveaux enjeux ? », *Lettre Innovation et Prospectives*, n° 05, juillet 2013.

directive 95/46/CE et ensuite par le Règlement (UE) 2016/679, est de s'appuyer sur des définitions larges, non-tributaires des instruments techniques utilisés, selon le principe de neutralité technologique. Procéder ainsi permet en théorie de pouvoir réglementer le plus de situations juridiques possibles, sans se soucier pour autant des évolutions technologiques qui auraient pu venir limiter la portée du texte[190].

75. L'écosystème de l'automesure connectée, composé de différents objets techniques, applications ou encore serveurs de stockage, est rendu viable grâce à l'interconnexion des différents dispositifs utilisés. L'enjeu du sujet est donc de pouvoir, malgré la multiplication des opérations de traitements réalisées par les différents dispositifs, réussir à caractériser juridiquement les données qui en sont issues. Ce travail de définition est essentiel car il permet de déterminer le spectre des informations qui sont collectées par la pratique de l'automesure et ainsi de savoir quelle protection leur apporter, malgré l'apparente diversité des dispositifs utilisés.

Deux catégories de données, définies respectivement aux articles 2 et 6 de la loi Informatique et Libertés réécrite ainsi qu'aux articles 4 et 9 du Règlement général européen, semblent ainsi collectées par les différents dispositifs d'automesure. Les données récoltées par les objets et dispositifs connectés de quantified-self s'apparentent en effet à des données à caractère personnel classiques, telles qu'elles sont définies par la réglementation **(section 1)**. Mais l'automesure connectée, fondée sur la mesure du bien-être et d'éléments relatifs au corps humain et à l'activité physique, favorise également la collecte de données sensibles relatives, dans certains cas, à la santé **(section 2)**.

[190] G 29, *Avis 4/2007 sur le concept de données à caractère personnel*, 01248/07FR WP 136, adopté le 20 juin 2007.

SECTION I – LE *QUANTIFIED-SELF*, PRATIQUE PERMETTANT LA COLLECTE DE DONNÉES PERSONNELLES

76. La définition juridique actuelle des données personnelles est fondée sur celle issue de la loi Informatique et Libertés telle qu'elle avait été modifiée par la transposition de la directive 95/46/CE du Parlement européen et du Conseil[191]. Celle-ci reflétait la volonté du législateur européen d'adopter une définition large des données personnelles. La proposition modifiée de la Commission indiquait déjà à l'époque qu'il fallait « adopter la définition la plus globale possible de la notion de données à caractère personnel, afin de couvrir toutes les informations qui peuvent être reliées à une personne physique »[192]. Cette position, identique à celle du Conseil dans la position commune[193], révélait ainsi la volonté d'intégrer un grand nombre d'informations au sein de la définition retenue.

Également développé par la Convention 108 du Conseil de l'Europe[194], le champ d'application de cette définition n'a pas changé avec l'adoption du Règlement général européen[195]. Reprenant les mêmes termes que ceux employés par la directive de 1995, celui-ci propose une conception extensive des informations personnelles ayant vocation à être protégées. L'intérêt de cette définition est de ne pas être limitée par les nouvelles avancées technologiques. Celle-ci va donc pouvoir s'appliquer sans considération du support permettant de recueillir la donnée **(§1)** et la pratique de l'automesure va faciliter sa mobilisation **(§2)**.

[191] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[192] COM (90), 422 final, Proposition modifiée de directive 95/46, 15 octobre 1992.
[193] Position commune (CE) nº 1/95 arrêtée par le Conseil le 20 février 1995, JO C 93 du 13 avril 1995, p. 20.
[194] Convention 108 du Conseil de l'Europe, pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28. I.1981.
[195] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

§1. Une qualification indépendante du moyen de collecte

77. L'ensemble de l'arsenal législatif relatif à la protection des données personnelles est pensé dans le but de régir des situations diverses et qui n'étaient parfois pas envisagées à l'origine. L'objectif recherché par le législateur est ainsi de permettre au cadre juridique de s'adapter aux différentes évolutions technologiques. L'étendue du spectre conféré à cette réglementation permet donc d'identifier et de qualifier juridiquement les données générées dans le cadre d'une activité de *quantified-self* et ce grâce à une définition étendue de la notion de donnée personnelle, laquelle a évolué depuis 1978 pour s'adapter aux développements du numérique et à l'apparition de nouveaux outils techniques[196].

La diversité des supports et outils numériques employés dans le cadre de l'automesure de soi n'a théoriquement pas d'incidences sur l'éventuelle qualification juridique des données qui en sont issues. Des éléments de distinction objectifs permettant une identification large des individus, personne physique, ont été déployés. Pourtant, malgré des critères de rattachement larges à la définition de donnée personnelle **(A)**, certaines situations et exceptions entrainent l'exclusion de ces données du régime protecteur mis en œuvre par la loi **(B)**.

A. Les critères de qualification d'une donnée personnelle

78. L'article 2 de la loi Informatique et Libertés indique, par renvoi au Règlement européen, quels sont les éléments permettant de retenir la qualification de donnée à caractère personnel telles qu'elles ont vocation à être collectées par des dispositifs d'automesure. Précisément définis, ces critères impliquent une identification de la personne, cette identification pouvant être directe **(1)**, mais également indirecte **(2)**.

[196] Voir notamment : Alexandre Maitrot de la Motte, « La réforme de la loi informatique et libertés et le droit au respect de la vie privée », *AJDA*, 2004, p. 2269 ; Jessica Eynard, *Essai sur la notion de données à caractère personnel*, Thèse, Toulouse I, 2011, 444 p. ; Alain Rallet, Fabrice Rochelandet, « La régulation des données personnelles face au web relationnel : une voie sans issue ? », *Réseaux 2011/3*, n° 167, p. 17 à 47 ; Frédérique 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.

1. Identification directe d'une personne physique

79. Des informations nominatives aux données à caractère personnel. La définition retenue par l'article 2 de la loi Informatique et Libertés, issue de la directive de 1995 et reprise par le Règlement général, est plus large et plus précise que celle proposée par la loi de 1978 dans sa rédaction initiale[197]. Alors que celle-ci traitait initialement des « informations nominatives », la loi de transposition du 6 août 2004 a acté le passage à l'emploi du terme de « données à caractère personnel ». Cette transition n'était pas neutre car elle a permis de prendre en compte la valorisation progressive attachée à la donnée[198]. Surtout, elle a entraîné une extension du champ de la protection par rapport à la loi de 1978 en permettant notamment une meilleure prise en compte des progrès des techniques d'identification[199].

En effet, le passage des « informations nominatives » aux « données à caractère personnel » vient élargir le champ des situations susceptibles d'être régies par la réglementation. L'identification d'une personne ne suppose plus nécessairement « l'association formelle d'un visage et d'un nom »[200] mais englobe toutes les données permettant d'identifier une personne, qu'il s'agisse d'un nom, d'un numéro d'identification, de la voix, d'images ou encore des empreintes digitales. Tous les éléments relevant de l'identité de la personne sont désormais inclus dans la définition élargie, qui est également celle retenue à l'article 4 du Règlement général européen.

80. La modification de la nature des données. Une telle extension du champ des données concernées par la loi Informatique et Libertés est révélatrice des « modifications de la nature des données et des informations qui se rapportent aux individus à l'ère du numérique »[201]. Les outils techniques utilisés pour collecter des

[197] Marie-Claire Ponthoreau, « La directive 95/46/CE 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 », *RFDA*, 1997, p. 125.
[198] Frédérique 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.
[199] Guy Braibant, *Données personnelles et société de l'information*, Rapport au Premier Ministre sur la transposition en droit français de la directive n° 95/46, remis le 3 mars 1998.
[200] Marie-Claire Ponthoreau, *op. cit.*, p. 125.
[201] Commission de réflexion et de propositions *ad hoc* sur le droit et les libertés à l'âge du numérique, Rapport Numérique et libertés : un nouvel âge démocratique, n° 3119 déposé le 9 octobre 2015 par M. Christian Paul et Mme Christiane Féral-Schuhl, co-Présidents de la Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique, au nom de cette commission.

données sont de plus en plus performants et ceux-ci permettent une récolte de données de plus en plus variées. La formulation large retenue pour la définition des données à caractère personnel permet donc d'inclure à la fois une quantité importante de données mais elle permet également de s'affranchir de ces outils technologiques nouveaux utilisés pour la collecte en s'adaptant à leur apparition et à leurs éventuelles évolutions.

Ainsi, aux termes de l'article 4 du RGPD, une donnée à caractère personnel est « toute information se rapportant à une personne physique identifiée ou identifiable ». Concernant l'objet de l'information d'abord, celle-ci doit être relative à une personne physique, ce qui implique l'exclusion des personnes morales, ces dernières ne pouvant revendiquer un droit à la protection de leurs données à caractère personnel. Concernant ensuite la qualité de l'information, celle-ci doit permettre l'identification de cette personne physique. Or, comme l'indiquent les différents textes, cette identification peut être réalisée de deux façons : directement et indirectement.

81. La directive de 1995 a apporté certaines précisions sur ce point, qui ont été reprises par la suite[202]. Elle a notamment indiqué que l'on retrouve, parmi les données personnelles, celles qui sont « propres à l'identité physique, psychique, économique, culturelle ou sociale »[203]. La jurisprudence a eu l'occasion de faire application de ces différents critères, notamment concernant des informations telles que le nom et le prénom[204], les coordonnées postales ou téléphoniques[205] ou encore les coordonnées électroniques[206]. L'élargissement des différents critères de rattachement correspond ainsi au développement de nouvelles technologies modifiant le rapport à l'identité sur les réseaux numériques[207].

82. La pratique du *quantified-self* s'inscrit aujourd'hui dans le prolongement de cette modification de l'identité numérique. En dehors du recours éventuel à un pseudonyme, les critères identifiés ont pleinement vocation à s'appliquer. En effet, en

---

[202] Romain Perray, *JurisClasseur Administratif*, Fascicule 274-10 : Informatique. – Données à caractère personnel. – Introduction générale et champ d'application de la loi « Informatique et libertés », 30 juillet 2014, mise à jour du 31 mai 2015.
[203] Article 2, directive 95/46/CE.
[204] T. com. Paris, 1re ch., 28 janv. 2014, *M. X. c/Google Inc. et Google France*.
[205] CE, 11 avr. 2014, n°348111, *Juricom et associés c. CNIL*, inédit au recueil Lebon.
[206] Cass. Crim., 14 mars 2006, pourvoi n° 05-83.423, *Bull. crim*. N° 69.

utilisant un service connecté capable de collecter des données, un individu va être amené à interagir avec ce service en renseignant éventuellement – *a minima* – son nom, ses coordonnées ou encore ses informations électroniques, sans compter celles qui seront relevées automatiquement par le service.

Par ailleurs, la réglementation indique que pour « déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable de traitement ou toute autre personne »[208]. Dès lors, la simple possibilité de distinguer une personne n'est pas suffisante pour considérer que celle-ci est identifiable. L'identification doit en effet être réalisée avec certitude. Le considérant 26 du Règlement général européen précise cette exigence en faisant référence aux moyens « raisonnablement » susceptibles d'être mis en œuvre pour identifier la personne. Compte tenu des critères objectifs mentionnés pour déterminer le caractère raisonnable, tel que le coût de l'identification et le temps nécessaire à celle-ci, l'utilisateur d'un service de *quantified-self* sera aisément identifiable par la personne chargée du traitement, étant donné les informations qui seront directement transmises pour le bon fonctionnement du service.

Les éléments renseignés ou obtenus ne permettent pas toujours d'identifier directement l'individu. Mais, l'identification indirecte d'une personne permet également de retenir la qualification de donnée à caractère personnel.

2. Identification indirecte d'une personne physique

83. Outre les informations qui permettent d'identifier directement une personne, sont également comprises dans la notion de données à caractère personnel celles qui permettent l'identification indirecte de l'individu. On constate à nouveau le caractère large de la notion de données à caractère personnel, qui permet d'inclure

[207] Cf., *supra*, n°25.
[208] Article 2, loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée en 2004.

des éléments qui sont indirectement nominatifs. Déjà en 1994, la CNIL insistait sur la nécessité d'élargir le champ des données visées par la définition initiale[209].

84. Une évolution nécessaire. Cette vision large de la donnée à caractère personnel, dont l'évolution a été rendue nécessaire par le développement de la technologie, permet d'englober un nombre important de situations. En effet, les données personnelles « ne peuvent plus être considérées comme des entités autonomes à la manière des fiches individuelles cartonnées des fichiers du XXème siècle »[210]. La définition des données à caractère personnel a donc dû évoluer pour prendre en compte le déploiement de nouveaux outils technologiques ; l'intégration des informations indirectement identifiantes permet à la réglementation de s'adapter au développement de nouvelles traces numériques et donc d'inclure des éléments indirectement nominatifs.

La notion d'identification indirecte joue alors le rôle de correctif au cas où l'identification directe de l'individu serait impossible. Sortir du cadre restreint des données d'identification ou descriptives courantes que sont le nom, l'adresse ou encore l'appartenance à une catégorie socioprofessionnelle permet à la réglementation d'être évolutive et surtout de s'adapter, en théorie, aux avancées technologiques. Par exemple, les outils permettant de recueillir automatiquement des données lors de la connexion à certains services, tels que les fichiers *logs* - fichiers textes enregistrant de façon chronologique les opérations réalisées par une application informatique - sont désormais inclus dans cette définition[211].

La prise en compte des données issues du *quantified-self* semble donc favorisée par cette conception large de la définition. En effet, un individu ne renseignant pas forcément son nom, son prénom ou son adresse, verrait tout de même d'autres données le concernant, permettant indirectement son identification, être protégées. Les données relatives à la géolocalisation, au poids ou encore à l'indice de masse corporelle dans le cas d'un *tracker* d'activité, bracelet connecté équipé de

[209] CNIL, délib. n° 94-095, 15 novembre 1994.
[210] Rapport Numérique et Libertés, *op. cit.*, p. 115.
[211] Voir notamment : Audrey Yayon-Dauvet, « Le devenir de la protection des données personnelles sur Internet », *Gazette du Palais*, n° 256, 13 septembre 2001, p. 2 ; TGI Paris, Ordonnance de référé, 17 juillet 2014, *Chantal M. / Crédit Lyonnais*.

capteurs et porté directement par l'individu, sont tout particulièrement susceptibles de permettre cette identification indirecte. Ainsi, les pistes relatives à l'identification qui ont été proposées par la directive et qui sont complétées par le RGPD ont spécifiquement vocation à s'appliquer dans le cadre de l'automesure connectée[212].

85. L'adresse IP. Parmi les données permettant l'identification indirecte de l'individu, l'adresse IP, numéro unique d'identification attribué à un dispositif connecté au réseau Internet, est probablement celle qui a le plus fait débat ces dernières années. Cette assimilation à une donnée à caractère personnel de l'adresse IP a été réalisée par certaines juridictions judiciaires sur le fondement de l'ancien article 2 al. 2 de la loi Informatique et libertés[213]. Mais, cette analyse n'a cependant pas toujours fait l'unanimité. De nombreuses juridictions ont en effet considéré que l'adresse IP ne pouvait être considérée comme une donnée à caractère personnel[214] en raison notamment de l'impossibilité d'identifier directement l'auteur de la connexion[215] ou du fait que seule une personne autorisée pouvait obtenir indirectement l'identité de l'utilisateur via le fournisseur d'accès[216].

La Cour de justice de l'Union européenne a rendu le 24 novembre 2011 un arrêt affirmant que les adresses IP étaient des « données protégées à caractère personnel, car elles permettent l'identification précise desdits utilisateurs »[217]. Cette interprétation, s'inscrivant dans la lignée des positions adoptées respectivement par la CNIL depuis 2007[218] et par le Conseil constitutionnel en 2009[219], a été confirmée par une nouvelle décision de la Cour de justice de l'Union européenne en date de 2016

[212] Sur ce point, la directive 95/46/CE précisait que l'identification pouvait être réalisée « par référence à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ». Le Règlement (UE) 2016/679 a permis l'ajout de la notion d'identité « génétique ».
[213] TGI Bobigny, 14 décembre 2006, *Laurent F. / Sacem*.
[214] TGI Bayonne, 15 nov. 2005, confirmé par CA Pau, 24 août 2006 ; TGI Paris, 24 déc. 2007.
[215] CA Paris, 15 mai 2007, n° 06/01954.
[216] CA Paris, 28 mai 2008, n° 2007-01064.
[217] CJUE, 24 novembre 2011, G. Ch., *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, *Dalloz actualité*, 29 nov. 2011, obs. C. Manara ; D. 2012. 2343, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; *ibid*. 2836, obs. P. Sirinelli ; *RSC* 2012. 163, obs. J. Francillon ; *RTD eur*. 2012. 404, obs. F. Benoît-Rohmer ; *ibid*. 957, obs. E. Treppoz
[218] Sur ce point, voir : https://www.cnil.fr/fr/ladresse-ip-est-une-donnee-caractere-personnel-pour-lensemble-des-cnil-europeennes
[219] CC, décision n° 2009-580 DC du 10 juin 2009, *Loi relative à la diffusion et à la protection de la création sur Internet*.

affirmant qu'une adresse IP dynamique, différente d'une adresse IP fixe car différente à chaque connexion, est une donnée à caractère personnel[220].

86. La Cour de cassation a également affirmé, dans un arrêt en date du 3 novembre 2016, que « les adresses IP, qui permettent d'identifier indirectement une personne physique, sont des données à caractère personnel, de sorte que leur collecte constitue un traitement de données à caractère personnel et doit faire l'objet d'une déclaration préalable auprès de la CNIL. »[221]. Cette affirmation vient non seulement s'inscrire dans la lignée de ce qui était affirmé à l'origine par certains juges du fond[222] mais elle est également conforme à la solution préconisée par le règlement européen[223].

Cette assimilation de l'adresse IP à une donnée à caractère personnel n'est pas sans incidence sur le domaine du *quantified-self*. Certains des outils numériques utilisées pour sa pratique sont effectivement dotés d'une adresse IP qui permet d'identifier indirectement l'individu. Il s'agit notamment des cas où une application est téléchargée et utilisée directement sur un *smartphone* ou bien une tablette. Dans ce cas, l'adresse IP associée au dispositif connecté permet en effet d'identifier indirectement l'utilisateur. Il était donc nécessaire que celle-ci soit incluse dans les différents cas de figure prévues par la réglementation. Ainsi conçue de manière extensive, la qualification de donnée à caractère personnel doit pourtant être exclue dans certains particuliers.

B. Les critères d'exclusion de la qualification de données personnelles

87. Il est désormais établi que la définition des données personnelles reflète une volonté d'y rattacher un nombre toujours plus grand d'informations. Pourtant, certains cas d'espèce font figure d'exceptions et nécessitent, pour des raisons pratiques, que ne soit pas appliquée la loi Informatique et Libertés ou le RGPD. Certaines données sont par nature non-identifiantes **(1)** et le cadre de l'activité purement domestique, parce qu'il n'implique aucune communication à des tiers,

[220] CJUE, 19 oct. 2016, 2ème Ch., *Patrick Breyer c. Bundesrepublik Deutschland*, C-582/14.
[221] Cass. 1re civ., 3 novembre 2016, pourvoi n° 15-22.595 (à paraître).
[222] TGI Saint-Brieuc, 6 septembre 2007, *Ministère public, SCPP, SACEM c/ J.-P.*

permet d'écarter l'application de la réglementation relative aux données personnelles **(2)**.

1. Les données non-identifiantes

88. Une hypothèse rare. Compte-tenu du caractère englobant de la définition actuelle de donnée à caractère personnel, peu de données sont susceptibles d'échapper à cette qualification, notamment dans le cadre du *quantified-self*. Le caractère toujours plus large des critères d'identification établis rend en effet difficile l'appréhension de données non-identifiantes ; il subsiste ainsi de moins en moins de données qui, par nature, ne permettent pas de révéler l'identité d'un individu et qui ne peuvent donc pas être reliées, directement ou indirectement, à une personne physique. Une donnée relative à l'horaire ne permet pas, par exemple, d'identifier l'individu. Mais il sera pourtant possible, dans certains cas, d'établir un lien avec la personne lorsque cette donnée est rapprochée d'autres informations[224].

89. La pratique de l'automesure contribue également à redéfinir la notion de donnée à caractère personnel : une donnée, intégrée à l'écosystème de l'automesure, est susceptible, par croisement ou corrélation, d'entraîner l'identification de la personne. Les mécanismes d'interconnexion de données[225], favorisés par les dispositifs d'automesure utilisés, influencent donc également la notion même de donnée à caractère personnel, telle qu'elle est définie par la LIL. Une donnée relative au poids, renseignées dans une application de *running*, ne rend pas possible l'identification d'un individu. Mais cette identification est facilitée lorsque la donnée est cumulée avec d'autres informations relatives à la taille et à l'âge. Toute information, pouvant désormais faire l'objet de croisements et de rapprochements, devient potentiellement donnée à caractère personnel, entraînant ainsi l'application du régime juridique protecteur.

---

[223] Sur ce point, voir le considérant (30) du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.
[224] Cf., *infra*, n° 572.
[225] Cf., *infra*, n° 158.

90. Le cas de l'anonymisation. Le spectre des données non identifiantes peut sembler résiduel au regard de l'ensemble des informations traitées[226]. Pourtant, les différents textes ont progressivement identifié une catégorie de données pouvant faire exception à l'application de la réglementation. La directive de 1995 visait à l'origine les « données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable »[227]. Cette solution a été reprise et complétée par le RGPD. Celui-ci indique en effet « qu'il n'y a […] pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. Le présent règlement ne s'applique par conséquent pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche »[228].

La logique mise en œuvre par cette disposition est aisément compréhensible. Elle permet d'écarter l'application de la réglementation Informatique et Libertés lorsque des données, susceptibles d'être directement ou indirectement identifiantes, sont anonymisées. Une précision doit cependant être apportée : les données dont il est ici question ont pu, avant leur anonymisation, être considérées comme étant des données à caractère personnel au sens classique de la définition. Ce n'est en effet qu'après une opération technique permettant de procéder à l'anonymisation que l'on va considérer que les données ne sont plus identifiantes et donc que l'application de la réglementation peut être écartée. Les données vont donc perdre leur statut de données à caractère personnel après l'opération d'anonymisation, cette dernière imposant que l'identification, directe ou indirecte, soit rendue impossible. Les dispositifs d'automesure ne permettent généralement pas cette anonymisation lors du traitement initial, l'activité étant directement traduite en donnée. Mais les informations peuvent ensuite être anonymisées par le responsable de traitement, lorsque des opérations ultérieures sont réalisées. A cette exception, fondée sur une

[226] Romain Perray, Julie Uzan-Naulin, « Existe-t-il encore des données non personnelles ? », *Dalloz IP/IT*, 2017, p. 286.
[227] Considérant 26, Directive 95/46/CE.
[228] Considérant 25, Règlement (UE) 2016/679

opération technique, s'en ajoute une relative au cadre domestique des opérations réalisées.

2. Le cadre de l'activité purement domestique

91. La loi Informatique et Libertés précise, dans son article 2, que celle-ci n'a pas vocation à s'appliquer lorsque les traitements sont « mis en œuvre pour l'exercice d'activités strictement personnelles ou domestiques »[229]. La directive de 1995 précisait déjà qu'il s'agissait des activités dites « domestiques » [230] et le considérant 18 du Règlement général européen vient étoffer cette définition en précisant qu'il s'agit des activités « sans lien avec une activité professionnelle ou commerciale ». Le RGPD précise également certains exemples en indiquant que figurent potentiellement, parmi ces activités, « l'échange de correspondance et la tenue d'un carnet d'adresses, ou l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités »[231].

Les raisons qui poussent à l'adoption de telles exceptions sont également compréhensibles. Un individu doit pouvoir manipuler des données à caractère personnel dans un cadre purement privé sans être tenu par l'ensemble des règles de la loi Informatique et Libertés. C'est d'ailleurs la position qui avait été adoptée par le groupe de l'article 29 au sein de son avis sur les récentes évolutions relatives à l'Internet des objets. Celui-ci a explicitement indiqué que « si les données qu'ils [les utilisateurs] collectent et mémorisent sont exclusivement utilisées à des fins personnelles ou domestiques, ils relèvent de « l'exemption domestique » visée dans la directive 95/46 »[232]. Un individu qui utilise une montre connectée pourra ainsi choisir de ne pas synchroniser les informations collectées avec d'autres applications. Les informations, collectées à titre purement indicatif, ne feront pas l'objet d'analyse ultérieures.

---

[229] Article 2 de la loi Informatique et Libertés du 6 janvier 1978 modifiée par l'ordonnance du 12 décembre 2018.
[230] Considérant 12, Directive 95/46/CE.
[231] Considérant 18, Règlement (UE) 2016/679.
[232] G 29, *Avis 8/2014 sur les récentes évolutions relatives à l'internet des objets*, 1471/14/FR WP 223, adopté le 16 septembre 2014.

92. Dès lors, un dispositif connecté qui ne transmet aucune donnée hors de l'appareil doit être considéré comme procédant à un traitement relevant de l'exemption domestique. Cette conclusion semble particulièrement adaptée au cas du *quantified-self*. Un individu utilisant par exemple un *tracker* d'activité afin de suivre le nombre de pas parcourus chaque jour n'a pas forcément vocation à transférer ces informations sur un autre support. Les informations collectées ne sont donc pas transmises hors du dispositif et le traitement réalisé bénéficie de l'exemption domestique permettant d'écarter l'application du dispositif protecteur de la loi Informatique et Libertés.

Cette solution semble justifiée dès lors que le traitement est réalisé par l'individu mais une nuance doit cependant être apportée au cadre de l'exemption domestique. Le traitement peut en effet être réalisé par l'individu à des fins exclusivement personnelles. Cependant, fabricants du dispositif connecté ou éditeurs de services peuvent également traiter conjointement les données personnelles de ce dernier. Dans ce cas, plusieurs distinctions doivent être réalisées pour déterminer le rôle exact de chacune des parties en présence. Lorsque des données sont collectées directement par le fabricant ou l'éditeur de service, celui-ci endosse directement la qualification de responsable de traitement, comme l'indique le Règlement européen. Ce dernier vient effectivement s'appliquer « aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques ». En revanche, si le service (hébergement, fonctionnalités supplémentaires, réseau social) est « uniquement réalisé au profit exclusif de l'utilisateur, alors le fabricant intervient plus comme un « sous-traitant » que comme un responsable de traitement à part entière »[233]. Dès lors, celui-ci se verra appliquer le régime juridique relatif au sous-traitant alors que l'utilisateur du dispositif permettant de procéder à l'automesure, considéré comme le responsable de traitement, pourra se soustraire aux dispositions de la réglementation.

La définition de donnée à caractère personnel fait, depuis son apparition, l'objet d'évolutions constantes lui permettant de couvrir un nombre toujours plus

[233] AFCDP, *Quantified Self connecté et Informatique & Libertés*, Synthèse des travaux du sous-groupe « Quantified Self », du groupe de travail « Données de santé » de l'AFCDP, Novembre 2015, p. 14.

important de situations. La pratique de l'automesure a une influence sur cette définition et celle-ci favorise également, par la nature des informations traitées et par la diversité des dispositifs utilisés, le recueil de données à caractère personnel.

§2. Une qualification favorisée par le moyen de collecte

93. La définition objective des données personnelles – telle que présentée précédemment – permet déjà d'inclure une quantité importante d'informations. Mais le moyen de collecte utilisé vient parfois favoriser et élargir le processus de récolte des données. Les objets connectés utilisés pour la pratique de l'automesure, directement portés par l'individu, permettent un recueil d'informations relatives à l'activité physique et au corps. Le *quantified-self*, visant à une meilleure connaissance de soi par la quantification de son activité, repose donc sur un croisement exponentiel de données **(A)** et permet dans le même temps le développement de traces numériques difficilement contrôlables par le sujet de la collecte de données **(B)**.

A. Le *quantified-self*, outil favorisant le croisement de données

94. La particularité du *quantified-self*, au regard de la réglementation Informatique et Libertés, est de permettre une collecte toujours plus importante de données de nature variée. Une telle collecte d'informations est généralement réalisée dans le but de suivre l'évolution de constantes relatives au bien-être. Il s'est donc avéré nécessaire de pouvoir prendre en compte les capacités de profilage permises par de tels instruments **(1)** et les éventuels cas de recoupement d'informations ont également été pris en compte par la réglementation **(2)**.

1. La prise en compte du profilage

95. Une reconnaissance progressive. La loi Informatique et Libertés précisait auparavant, dans son article 10, qu'un traitement automatisé de données à caractère personnel destiné à « définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité » ne pouvait servir de fondement à une décision produisant des effets juridiques à l'égard d'une personne. Le terme de profilage n'était pas directement

employé par le texte mais les effets produits étaient les mêmes que ceux résultant d'une opération de profilage. Il s'agissait en effet, à partir de données dites agrégées et donc regroupées par catégories, de déterminer un profil type de l'individu. La directive de 1995, à l'origine de l'article 10 de la loi, ne parlait pas non plus en tant que tel du profil. Celle-ci faisait simplement mention du traitement automatisé « destiné à évaluer certains aspects de sa personnalité ». Malgré cette absence de consécration directe par la législation, cette « intrusion dans la sphère privée » qui est impliquée par le profilage a rapidement nécessité que sa définition soit précisée[234].

96. La consécration par le RGPD. La doctrine, pour définir le profilage, s'attachait auparavant à sa finalité. Faisant référence à la question de l'utilisation d'algorithmes ou encore à la surveillance[235], celle-ci ne proposait pourtant pas de définition unifiée de la notion. L'article 4 du règlement général est venu combler ce vide et celui-ci indique désormais qu'il s'agit de « 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 ». Les adaptations successives du cadre juridique national au droit européen en juin et décembre 2018 ont permis l'intégration de la notion à l'article 47 de la LIL qui fait désormais explicitement référence au profilage. En matière de données dites sensibles, l'article 95 de la loi interdit le profilage qui entraînerait une discrimination des individus.

La consécration d'une telle notion répond au besoin de protéger les individus des risques induits par un traitement toujours plus important de données personnelles. En effet, l'identification des « habitudes de vie très précises pouvant générer des risques de discrimination »[236] que permet le profilage se trouve exacerbée par

[234] Gérard Haas, Amanda Dubarry, « Confidentialité et protection des données », *Dalloz IP/IT*, 2017, p. 322.
[235] Mireille Hildebrandt, Serge Gutwirth, *Profiling the European Citizen : Cross-Disciplinary Perspectives*, Springer, 2008, p. 17. V. égal. : *The Dawn of a Critical Transparency Right for the Profiling Era*, Amsterdam, Digital Enlightenment Yearbook, 2012, p. 212.
[236] Célia Zolynski, « La Privacy by Design appliquée aux Objets Connectés : vers une régulation efficiente du risque informationnel ? », *Dalloz IP/IT*, 2016, p. 404.

l'utilisation d'objets connectés dans le cadre du *quantified-self*. Un individu fournissant en permanence des éléments relatifs à son mode de vie, tels que l'évolution de son poids, ses habitudes alimentaires, ses déplacements ou encore ses activités physiques, transmet justement des indications permettant de déterminer un profil. Ce quadrillage des activités de l'individu est d'ailleurs, dans certains cas, explicitement mentionné au titre des finalités et objectifs du *quantified-self*.

97. Une faculté encadrée. Ainsi, il ne s'agit pas d'interdire totalement la réalisation d'un profil de l'individu, mais simplement d'en limiter la portée et les effets. Une solution contraire aurait en effet pour conséquence l'impossibilité de mettre en œuvre un traitement d'automesure. Le RGPD précise que « la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage ». Plusieurs exceptions sont cependant prévues. Une telle disposition ne trouve pas à s'appliquer lorsque la décision est justement « nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement » ou encore, qu'elle est « autorisée par le droit de l'Union ou le droit de l'Etat membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ». Enfin, cette exception peut être également « fondée sur le consentement explicite de la personne concernée »[237]. Le contrat passé entre l'individu et le fournisseur du service d'automesure permettra ainsi d'encadrer la mise en œuvre d'une opération de profilage et le consentement de l'individu sera requis en l'absence de telles dispositions contractuelles. Le profilage ne fait donc pas l'objet d'une interdiction mais il est strictement encadré afin de préserver les droits des individus. Une telle constatation peut également être opérée pour le cas où il serait possible de recouper des données afin d'en déduire des informations identifiantes.

2. Les cas de recoupement des informations

98. Dans le prolongement des informations permettant une identification indirecte de l'individu et de celles permettant de dresser un profil, le cas des

situations visant à recouper des informations afin d'en extraire des données identifiantes mérite également d'être mentionné. Une donnée doit objectivement permettre d'identifier un individu. Mais il existe pourtant des situations, fréquentes dans le cadre de l'automesure, dans lesquelles c'est en procédant à un recoupement d'informations qu'il sera possible de procéder à une telle identification.

99. L'étude des circonstances. Théoriquement, l'identification « se fait normalement au moyen d'informations spécifiques que l'on peut appeler identifiants et qui présentent une relation particulièrement privilégiée et étroite avec la personne physique concernée ». Pourtant, « le contexte particulier et les circonstances liées à un cas spécifique sont déterminants dans cette analyse »[238]. Dès lors, pour savoir si des informations peuvent véritablement se rapporter à un individu, il se révèle essentiel de procéder à une étude des circonstances dans lesquelles ces informations sont collectées.

L'exemple le plus couramment évoqué est celui relatif au nom de famille. Ainsi, comme l'indiquait le groupe de l'article 29, « un nom de famille très courant sera insuffisant pour identifier quelqu'un […] alors qu'il sera probablement suffisant pour identifier un élève dans une classe »[239]. La jurisprudence a d'ailleurs eu l'occasion de faire application de ce principe en matière de résultats des examens du permis de conduire. Elle a considéré que le registre ayant pour finalité la gestion des examens, contenant simplement les noms des individus, ne comportait aucune donnée nominative[240].

100. L'accumulation de données. La CNIL a pourtant adopté une solution différente à propos des données traitées par les différents services de la société Google. En effet, même si prises isolément, les données – telles que des identifiants – ne permettent pas toujours d'être « automatiquement considérées comme directement identifiantes » car ne se rapportant qu'au seul terminal ou navigateur de l'utilisateur, « l'accumulation de données que cette société détient sur une seule et même personne

---

[237] Article 22, Règlement (UE) 2016/679.
[238] Avis 4/2007 sur le concept de données à caractère personnel, précité, p. 14.
[239] *Ibid.*

lui permet de la singulariser à partir d'un ou de plusieurs éléments qui lui sont propres »[241]. Une telle solution est aisément compréhensible, au regard des finalités initiales de la loi Informatique et Libertés. Celle-ci ayant été adoptée afin de prévenir les cas d'interconnexion ou de mise en relation de fichiers et d'informations, la position adoptée par la CNIL s'inscrit dans la continuité de ce raisonnement et tend à prévenir au maximum les risques liés au croisement de données.

Comme il est rappelé dans cette délibération de la CNIL, « les législateurs européen et français ont consacré une conception large de la notion de donnée à caractère personnel, qui peut être directement ou indirectement identifiante ». La possibilité d'identifier une personne déterminée, à partir d'identifiants spécifiques ou d'un ou plusieurs éléments qui lui sont propres, conduit donc « à regarder ceux-ci comme des données à caractère personnel ». Il semble dès lors impossible de « ne pas considérer que celles-ci ne sont pas identifiantes, à tout le moins indirectement ». Si ce cas de figure présente certaines spécificités – matérialisées par le croisement de données entre les différents services proposés par la société Google – la solution n'en reste pas moins pertinente à l'égard du *quantified-self*.

En effet, le cadre de l'automesure de soi facilite – par ses modalités – le croisement de données, étant donné que l'objectif pour l'utilisateur est de pouvoir collecter le plus d'informations possibles afin notamment de « routiniser » le processus d'une part et d'obtenir des mesures relatives à de nombreux facteurs d'autre part[242]. Dès lors, si une donnée issue d'un objet doté d'un capteur connecté est relative au poids de l'individu, celle-ci ne sera pas forcément suffisante pour identifier l'individu. Pourtant, couplée à une donnée relative à la taille, cette information devient plus précise et permet de faciliter l'identification de l'individu. Le même type de raisonnement peut être appliqué lorsque l'objet connecté utilisé permet de procéder à la géolocalisation de l'individu. Ces données ne sont pas

[240] CAA Douai, 1ère ch., 17 mai 2001, n° 99DA020329.
[241] CNIL, délib. n° 2013-420 du 3 janvier 2014 prononçant une sanction pécuniaire à l'encontre de la société X.
[242] CNIL, « Le *quantified-self* : nouvelle forme de partage des données personnelles, nouveaux enjeux ? », *Lettre innovation et prospective*, n° 05, juillet 2013.

directement identifiantes mais leur recoupement permet d'en conclure qu'elles sont des données personnelles.

B. Le *quantified-self*, outil favorisant le développement de traces numériques

101. Les nanotechnologies, qui sont employées pour le déploiement des objets connectés et qui permettent l'automatisation du *quantified-self*, sont au cœur de problématiques nouvelles. Elles permettent le passage d'une problématique de fichiers à une problématique dite de traces. Avec les objets connectés et applications utilisés pour relever différentes mesures, il est en effet possible de distinguer les informations qui sont divulguées volontairement et consciemment par l'individu – par le prisme de l'objet connecté ou d'une application – et les informations qui sont divulguées de manière involontaire dans le cadre des besoins techniques du service.

102. L'individu n'est pas toujours conscient de la masse de données qui est générée par le service qu'il utilise et qu'il transmet par la suite[243]. Parmi les données collectées, on retrouve donc celles qui sont délibérément transmises par l'utilisateur – par exemple, le nombre de calories ingérées en une journée par une personne – et également des données dites « passives » qui sont recueillies de manière automatique[244]. Tout aussi révélatrices de la vie privée des individus, ces données ont été progressivement prises en compte par les évolutions juridiques **(1)**, permettant ainsi de limiter théoriquement le déploiement de projections algorithmiques **(2)**.

1. La prise en compte des métadonnées

103. Les révélations opérées par Edward Snowden à propos de la surveillance réalisée par la NSA[245] ont permis de mettre en lumière le rôle des métadonnées dans le fonctionnement technique des services numériques. En effet, il n'était pas reproché

[243] Juliette Sénéchal, « La fourniture de données personnelles par le client via Internet, un objet contractuel ? », *AJ Contrats d'affaires, Concurrence, Distribution*, 2015, p. 212.
[244] Thierry Berthier, « Projections algorithmiques et cyberespace », *Revue internationale d'intelligence économique*, 5.2, 2013, p. 179 à 195.
[245] *National Security Agency*, agence de renseignement gouvernementale américaine créée en 1952 et affiliée au Département de la défense des Etats-Unis.

à l'agence de surveillance d'écouter directement les conversations des individus, mais de collecter des métadonnées, traces relatives aux communications électroniques (nom du destinataire, horaires de début et fin de communication, lieux où se situent les communicants)[246]. Définie par le dictionnaire Larousse comme une « donnée servant à caractériser une autre donnée, physique ou numérique », la notion de métadonnées n'a fait son apparition que récemment en droit.

A l'heure actuelle, le seul texte juridique proposant également une définition des métadonnées est le Code de l'environnement. Présentées à l'article L.127-1, 6° de ce dernier, elles y sont définies comme « des informations décrivant les séries et services de données géographiques et rendant possible leur recherche, leur inventaire et leur utilisation ». Assez proche de la définition générale précitée, on s'accorde de manière plus générale pour dire que le terme fait référence à des données sur des données, permettant de définir, circonscrire ou décrire une autre donnée. De nature variée, elles peuvent intégrer des durées, des dates, des lieux, des événements ou encore des éléments d'identification de la personne[247].

104. Une nature juridique imprécise. Les technologies génératrices de traces et exploitées par les objets connectés et les services en ligne montrent que les nouvelles « mémoires informatiques n'enregistrent plus nécessairement des identités, mais des traces électroniques, susceptibles d'être indirectement nominatives et de témoigner des faits et gestes de chacun »[248]. Les traces numériques, conscientes mais surtout inconscientes, posent la question de la nature juridique des métadonnées. En effet, celles-ci n'ont à l'origine pas vocation à révéler des informations directement en lien avec la vie privée des individus. Pourtant, certaines d'entre elles peuvent être considérées comme étant des données personnelles des utilisateurs lorsqu'elles sont susceptibles de permettre leur identification. Un individu utilisant un service en ligne

[246] David Lyon, *Surveillance after Snowden*, Polity Press, Octobre 2015, p. 120.
[247] Manuel Munier, Vincent Lalanne, Pierre-Yves Ardoy, Magali Ricarde, « Métadonnées et Aspects Juridiques : Vie Privée vs Sécurité de l'Information », *9ème Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information (SARSSI 2014)*, Mai 2014, Saint-Germain-au-Mont-D'or, France, 2014, p. 65 à 76.
[248] Bénédicte Rey, *La vie privée à l'heure du numérique*, Lavoisier, 2012, 304 p.

ou un objet connecté va dès lors émettre lui-même les signaux numériques permettant de le tracer[249].

105. Une nécessaire clarification. Prenant en considération ces différents développements, la proposition de règlement du Parlement européen visant à remplacer la directive « e-privacy »[250] entend clarifier la définition juridique de la notion de métadonnée et en donner une définition appliquée au domaine du numérique. Entendue de manière large, la définition fait notamment référence « aux données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques ». Inclure cette notion au sein de la réglementation Informatique et Libertés permettrait de considérer les métadonnées comme étant des données à caractère personnel. Ainsi, cela permettrait de pouvoir les identifier clairement et donc de pouvoir leur appliquer un régime juridique précis. Par ailleurs, cela contribuerait également à mieux protéger les données issues des projections algorithmiques permises par le *quantified-self*.

2. Le déploiement de projections algorithmiques

106. Comme cela a été précédemment indiqué, les *smartphones* et autres outils techniques numériques génèrent de plus en plus de métadonnées, correspondant à des informations précises qu'il est possible de rattacher à la vie privée des individus[251]. Les données collectées ne concernent pas directement le contenu des communications, mais celles-ci sont présentes en nombre suffisant pour « permettre de tirer des conclusions très précises concernant la vie privée des personnes telles que les habitudes de la vie quotidienne »[252]. Or, ces métadonnées, associées aux données directement fournies par l'utilisateur, viennent s'insérer dans un ensemble plus vaste

[249] Dominique Quessada, « De la sousveillance. La surveillance globale, un nouveau mode de gouvernementalité », *Multitudes*, 2010/1, n° 40, pp. 54-59.
[250] Proposition de Règlement européen du Parlement européen et du Conseil, concernant le respect de la vie privée et la protection des données à caractère personnelles dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »).
[251] Marine Farshian, « Quand la réalité de la surveillance massive tend à dépasser la fiction orwellienne », Droit à la vie privée et protection des données personnelles (Assemblée Parlementaire du Conseil de l'Europe), *La Revue des droits de l'homme*, Revue du Centre de recherches et d'études sur les droits fondamentaux, 2015.
[252] Sylvie Perrou, « La Cour de justice, garante du droit « constitutionnel » à la protection des données à caractère personnel », *RTD Eur.*, janvier-mars 2015, p.117.

intitulé projection algorithmique qui est rendu possible par le recours à des suites de calculs automatisés.

a. Une projection involontaire de données

107. Le concept de projection algorithmique a été défini comme un phénomène visant à décrire la production de données et de métadonnées résultant des interactions entre « un opérateur humain avec les systèmes qui l'entourent »[253]. Cette notion permet également de généraliser la notion de traces numériques produites volontairement ou non par un individu. A ce titre, une projection algorithmique est donc créée par l'interaction entre un réseau de capteurs et des objets connectés et l'on constate souvent que le volume de la projection algorithmique créée par un individu tend à dépasser celui de la projection volontaire[254]. Le nombre de données créées involontairement rien que par l'utilisation du service devient ainsi plus important que le nombre de données que l'individu souhaite consciemment créer et divulguer.

Cette projection algorithmique, qui est notamment le « résultat des capacités de corrélation des procédés d'analyse statistique » permis par les outils numériques, fait « entrer dans l'espace des données personnelles un ensemble de données fragmentées, en apparence anodines, qui en étaient jusqu'alors exclues »[255]. Présentant des similitudes avec les problématiques juridiques posées par les métadonnées, les projections algorithmiques viennent s'insérer dans la masse du *big-data* – ou des gros volumes de données dans sa traduction française – pour venir définir l'ensemble des signaux émis par une personne lors de son utilisation d'un objet numérique, sans égard pour le support technique utilisé.

108. Chacun des éléments composant cette projection algorithmique sont juridiquement définis et pris en compte : métadonnées identifiantes ou non, données directement et indirectement identifiantes, données non-identifiantes. Mais les capacités de corrélation et de croisement développées mettent à mal les catégories

[253] Thierry Berthier, « Projections algorithmiques et villes ubiquitaires », *Chaire de Cybersécurité & cyberdéfense Saint-Cyr Thales Sogeti*, Juillet 2015, article I.3.
[254] *Ibid.*
[255] Jean-Marc Deltorn, « La protection des données personnelles face aux algorithmes prédictifs », *RDLF*, 2017, chron. n°12.

juridiques prédéfinies lorsqu'il s'agit de saisir ces traces dans leur globalité[256]. En effet, les algorithmes – en tant qu'outils d'analyse statistique – permettent une interprétation de ces signaux numériques afin d'en extraire de nouvelles informations et notamment de prédire certains comportements. Or le *quantified-self* est particulièrement concerné par ce type de phénomène. Comme l'indique la CNIL, l'usage d'algorithmes prédictifs, suite de calculs automatisée visant notamment à prédire la survenance de situations, « permet de déduire des informations indirectes très intimes à partir d'une innocente collecte du nombre de pas ou d'une courbe de poids sur une longue durée »[257].

b. Une suite de calculs automatisés

109. Les objets connectés utilisés dans le cadre de l'automesure ont vocation à « désenclaver les mesures de leur enclos numérique pour se glisser dans les activités quotidiennes » [258]. Le recours à des algorithmes, notamment prédictifs, contribue à ce désenclavement et permet *in fine* une meilleure connaissance des individus. Dès lors, se pose la question de la qualification juridique à appliquer au phénomène algorithmique ainsi qu'aux projections qui en résultent, afin de pouvoir appliquer un régime permettant notamment de garantir le « caractère transparent et non-discriminatoire » des algorithmes[259]. Seule la loi pour une République numérique mentionne à l'heure actuelle directement la question des algorithmes et des traitements algorithmiques. Pourtant, bien qu'il ne soit pas directement mentionné par les différents textes dédiés spécifiquement à la protection des données, le régime juridique de l'algorithme doit être rapproché de celui du profilage. Il est en effet considéré comme l'un des moyens techniques permettant d'établir le profil de l'individu[260]. L'article 47 de la loi Informatique et Libertés ainsi que différents

[256] Luc-Marie Augagneur, « Vers des nouveaux paradigmes du droit dans l'économie numérique », *RTD Com*., 2015, p.455.
[257] CNIL, « Le corps, nouvel objet connecté », *Cahiers Innovation & Prospective*, n°2, mai 2014, 64 p.
[258] Dominique Cardon, *À quoi rêvent les algorithmes. Nos vies à l'heure des big data*, Paris, Seuil, La République des idées, 2015, p. 105.
[259] Jean-Philippe Foegle, « Le Conseil d'Etat, héraut de la révolution numérique ? », *La Revue des droits de l'homme*, [En ligne], Actualités Droits-Libertés, mis en ligne : 30 décembre 2014, consulté le 15 janvier 2016. URL : http://revdh.revues.org/1038.
[260] Conseil d'État, *Numérique et droits fondamentaux*, La Documentation française, 2014, p. 75.

considérants du RGPD font directement référence aux algorithmes, sans jamais les mentionner directement[261].

110. Certains en appellent aujourd'hui à la consécration directe d'un droit spécifique des algorithmes[262]. La présence en filigrane de cette notion dans la réglementation dote les individus d'une couche de protection supplémentaire contre les conséquences indésirables des traitements de données personnelles. Préciser la notion de traitement algorithmique et définir un régime juridique propre serait pourtant source de sécurité juridique pour les individus. La question des traces numériques laissées par les internautes lors de la navigation ou l'utilisation de services numériques, couplée à celle relative au traitement de données – personnelles ou non – par des algorithmes, est d'autant plus importante pour le développement du *quantified-self*. Celui-ci, par l'utilisation d'algorithmes et le croisement de différents types d'informations, favorise la collecte de données dites « sensibles » et touchant à l'intimité même de la personne.

Le cadre juridique relatif à la protection des données à caractère personnel, contenu au sein de la loi Informatique et Libertés et du RGPD, propose une définition large de la notion de donnée personnelle qui permet de qualifier juridiquement les informations traitées dans le cadre de l'automesure. Cette dernière, en procédant à la collecte d'informations relatives à l'activité physique et au corps humain, favorise également le recueil d'une catégorie particulière de données.

SECTION II. LE *QUANTIFIED-SELF*, PRATIQUE FAVORISANT LA COLLECTE DE DONNÉES SENSIBLES

111. Le *quantified-self* en tant qu'expression de l'Internet des objets, vient spécifiquement consacrer la numérisation et la quantification des activités humaines[263]. Ce faisant, ce mouvement de l'automesure de soi vient redéfinir la

[261] A ce titre, voir le considérant 24 qui mentionne notamment le fait de « prédire » des préférences.
[262] Lêmy D. Godefroy, « Pour un droit du traitement des données par les algorithmes prédictifs dans le commerce électronique », *Recueil Dalloz*, 2016, p. 438.
[263] Adam Thierer, « The Internet of Things and Wearable Technology : Addressing Privacy and Security Concerns without Derailing Innovation », *Richmond Journal of Law & Technology*, n°6, 2015.

relation que la personne entretient avec son corps en s'autoévaluant[264]. Surtout, il relève d'une exposition constante de soi et d'éléments relatifs à la vie privée et à l'intimité corporelle de la personne[265]. Ainsi, outre des données à caractère personnel soumises à un régime général, le *quantified-self* est susceptible de favoriser la collecte de données personnelles particulières, dites « sensibles » et hautement révélatrices d'éléments intimes.

A ce titre, la réglementation Informatique et Libertés énonce une liste limitative de données nécessitant une protection renforcée afin de garantir la protection de la vie privée de l'individu. Ces dernières sont soumises à un régime exorbitant du droit commun et font l'objet d'une protection théoriquement accrue. Leur spectre, aujourd'hui redéfini par la pratique de l'automesure, n'a pourtant pas toujours été facile à appréhender. La définition même des données dites « sensibles » a fait l'objet de certaines évolutions **(1)** pour progressivement prendre en compte le contexte de production de la donnée **(2)**.

§1. Une définition évolutive des données sensibles

112. L'article 8 de la loi Informatique et Libertés, avant sa réécriture par l'ordonnance de décembre 2018, indiquait qu'il était « interdit de traiter des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter 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 ». Le traitement particulier réservé à ce type de données, dont la liste a été complétée par la loi de juin 2018 et ensuite par l'ordonnance de réécriture du 12 décembre 2018, est aisément compréhensible : elles sont révélatrices d'informations particulièrement intimes.

---

[264] Dawn Nafus, Jamie Sherman, « Big Data, Big Questions| This One Does Not Go Up To 11 : The Quantified Self Movement as an Alternative Big Data Practice », *International Journal of Communication*, vol. 8, juin 2014, p. 11.
[265] Deborah Lupton, « Quantifying the body : monitoring and measuring health in the age of mHealth technologies », *Critical Public Health*, vol. 23, 2013.

113. Le *quantified-self* est spécifiquement concerné par cette notion. D'une part, la routinisation du processus en vue de l'efficacité des mesures relevées est évidemment susceptible de révéler des informations permettant une identification directe ou indirecte. D'autre part, le *quantified-self*, par la dimension « bien-être » et santé qui est développée, a par nature vocation à être alimenté par des données d'un genre particulier, entre données simplement relatives au bien-être et données de santé[266]. La définition de ces données sensibles est révélatrice d'une certaine ambivalence **(A)**, et l'on a progressivement assisté à un élargissement de la notion, permettant d'englober un important nombre de situations **(B)**.

A. Une définition ambivalente des données sensibles

114. Les données sensibles collectées et traitées dans le cadre du *quantified-self* recouvrent un spectre large. On distingue en effet, parmi les données personnelles sensibles traditionnelles, une catégorie de données spécifique et plus précise, relative explicitement à la santé des individus. La catégorie générale de données sensibles – définie dès l'origine par la réglementation – ne pose pas de problèmes particuliers d'interprétation. Son spectre large permet en effet d'inclure un nombre important de situations **(1)**. En revanche, les données personnelles relatives à la santé, intégrées au sein des données sensibles, ont longtemps dû faire face à une absence de définition, révélée notamment par les développements récents du *quantified-self* **(2)**.

1. Le spectre large des données dites « sensibles »

115. Une catégorie particulière de données. Dès 1978, la loi Informatique et Libertés crée une catégorie particulière de données, dites données « sensibles ». Sans pour autant en donner une définition précise, le texte énumère et identifie à ce moment dans son article 31 les données nominatives qui « directement ou indirectement font apparaître les origines raciales, les opinions publiques,

[266] Linda Ackerman, « Mobile health and fitness applications and information privacy », *Privacy Rights Clearinghouse*, San Diego, 2013, p. 2.

philosophiques ou religieuses ou les appartenances syndicales des personnes ». La mention des « mœurs des personnes » sera par la suite ajoutée[267].

La loi du 6 aout 2004 assurant la transposition de la directive 95/46 a intégré à cette liste les données relatives à la santé, mais également celles relatives à la vie sexuelle des individus[268]. Visant à remplacer l'ancienne notion de mœurs, elle se différencie de l'orientation sexuelle adoptée initialement par le projet de loi et jugée trop restrictive[269], bien que celle-ci soit désormais mentionnée par les dernières versions de la loi[270]. Surtout, elle permet de ne pas limiter le champ d'application à la question de l'homosexualité ou de la bisexualité, mais porte plus généralement sur des informations relatives aux pratiques sexuelles[271]. La loi du 20 juin 2018 modifiant la loi Informatique et Libertés a permis de compléter et de préciser cette notion, en mentionnant directement « la vie sexuelle ou l'orientation sexuelle d'une personne physique », tout comme l'ordonnance de réécriture de la loi du 12 décembre 2018.

116. La nécessité d'une protection renforcée. Cette liste de données sensibles – qui figure également au sein de l'article 6 de la Convention 108 du Conseil de l'Europe – permet de procéder à une catégorisation implicite des différents types de données concernées par la loi. La notion ne permet pas de procéder à une gradation de la sensibilité des informations collectées[272] mais elle permet d'identifier les informations dont le traitement est soumis à un régime particulier et à des garanties renforcées. Surtout, cette liste permet de définir un ensemble d'éléments considérés comme pouvant porter une atteinte particulière à l'intimité des individus. Ce risque renforcé d'atteinte, exacerbé par le développement de nouveaux outils techniques, justifie dès lors que ces données fassent l'objet d'une protection supplémentaire.

---

[267] Loi Informatique et Libertés, modifiée par la loi n°92-1336 du 16 décembre 1992, art. 257 JORF, 23 décembre 1992 en vigueur le 1er mars 1994, version en vigueur du 1 mars 1994 au 7 août 2004.
[268] Rapport n° 218 (2002-2003) de M. Alex Türk, fait au nom de la commission des lois, déposé le 19 mars 2003.
[269] *Ibid*., p. 59.
[270] Article 8 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.
[271] Romain Perray, *JurisClasseur Administratif*, Fascicule 274-10 : Informatique. – Données à caractère personnel. – Conditions de licéité des traitements de données à caractère personnel, 30 juillet 2014, mise à jour du 31 mai 2015.
[272] Danièle Bourcier, « Données sensibles et risque informatique, de l'intimité menacée à l'identité virtuelle », *Curapp*, Questions sensibles, Puf, 1998.

Protéger plus efficacement ces informations est en effet apparu essentiel, au vu des risques que leur révélation peut présenter. Qu'il s'agisse de la vie sexuelle, des croyances religieuses ou encore de l'appartenance politique, ces informations peuvent constituer une source de discrimination pour les individus, discriminations qui sont prohibées par l'article 225-1 du Code pénal. Il est dès lors nécessaire que ces données fassent l'objet d'un traitement particulier visant à limiter le nombre de personnes pouvant y avoir accès afin de limiter ces risques. Surtout, par le rattachement de ces données au régime juridique des données sensibles, les individus peuvent bénéficier de garanties de protection renforcées.

117. Le *quantified-self* est directement impacté par l'établissement de cette liste de données sensibles. De prime abord, les mesures opérées ou les objets connectés utilisés ne semblent pas pouvoir révéler certains éléments relatifs par exemple aux origines raciales, ethniques ou encore religieuses. Mais le rattachement à ce type de données peut n'être qu'indirect. Un individu qui suit son alimentation via une application pourra par exemple renseigner des mesures différentes lors d'une période de jeûne. Cette variation permettra de rattacher indirectement ce type de données à une confession religieuse[273]. Les applications permettant de suivre l'évolution d'un régime alimentaire sont par ailleurs susceptibles de révéler les croyances d'un individu par le renseignement d'aliments proscrits. Bien que ces applications n'aient pas pour finalité de révéler les croyances religieuses de l'individu, celles-ci sont donc susceptibles de le faire indirectement.

118. La catégorie des informations relatives à la vie sexuelle est également fortement impactée par le développement du *quantified-self* et par son automatisation via le déploiement des objets connectés. De nombreuses applications permettent en effet aujourd'hui de relever des mesures aussi variées que la fréquence, la durée ou encore l'intensité des rapports. Que ces informations soient recueillies directement par un objet connecté[274] ou que celles-ci soient renseignées manuellement par l'utilisateur dans le cadre d'une application[275], les données collectées permettent de

[273] Pour un exemple d'application permettant de tenir un journal alimentaire : https://www.myfitnesspal.com/fr
[274] https://aruco.com/2014/08/sexfit/
[275] https://itunes.apple.com/fr/app/sextrack/id431509019?mt=8

révéler des informations personnelles directement ou indirectement relatives à la vie sexuelle des individus.

Les données à caractère sensible recouvrent un nombre important d'informations relatives à l'intimité de la personne. Parmi celles-ci, les données personnelles relatives à la santé font l'objet d'une catégorie à part, caractérisée par son imprécision et par les difficultés d'interprétation de la notion.

2. L'absence de définition légale des données relatives à la santé

119. Le *quantified-self* touche directement le domaine de la santé en permettant par exemple de mieux vivre avec une maladie chronique grâce à une autosurveillance de son état de santé[276]. Un individu a ainsi la possibilité de numériser son activité physique, sans aucune médiation médicale[277]. Qu'il s'agisse en effet du cadre de la santé mobile ou de celui du *quantified-self* à proprement parler, les objets connectés ont permis, grâce à leur banalisation, un recueil facilité de données relatives à la santé des individus. Envisagées au titre des données sensibles nécessitant une protection particulière[278], les données de santé ont pourtant longtemps souffert d'une absence de définition légale, entraînant ainsi une acception mouvante de la notion.

120. Une distinction nécessaire. L'informatisation croissante des différentes étapes de parcours de soins ainsi que l'usage généralisé d'ordinateurs au sein de cabinets médicaux ont rapidement justifié que la notion de donnée de santé fasse l'objet d'une catégorie particulière au sein des données sensibles. Des régimes juridiques, applicables aux traitements ayant pour fin la recherche dans le domaine de la santé et l'évaluation des pratiques de soins et de prévention, ont été adoptés pour prendre en compte cette informatisation croissante de la santé. En contrepartie, l'article 8 de la directive de 1995, procédant en 2004 à une première réforme

[276] Emmanuel Gadenne, *Le guide pratique du Quantified Self. Mieux gérer sa vie, sa santé, sa productivité*, FYP éditions, juin 2012, Paris, 224 p.
[277] Renaissance Numérique, *D'un système de santé curatif à un modèle préventif grâce aux outils du numérique, 16 propositions pour un changement de paradigme des politiques de santé*, Livre Blanc rédigé sous la direction d'Henri Isaac, septembre 2014, 123 p.
[278] Guy Braibant, *Données personnelles et société de l'information*, Rapport au Premier Ministre sur la transposition en droit français de la directive n° 95/46, le 3 mars 1998, 292 p.

d'ampleur de la loi Informatique et Libertés de 1978, est venu inclure les données de santé aux « catégories de données dont le traitement est en principe interdit »[279].

121. Une absence de précision. Les données de santé, intégrant la liste des données sensibles tout en s'en distinguant à certains égards, ont donc fait l'objet d'une interdiction de traitement de principe. Une solution similaire a été adoptée par la Convention 108 du Conseil de l'Europe en son article 6. Pourtant, alors que ces textes indiquaient que cette catégorie de données nécessitait une protection particulière et que leur traitement devait faire l'objet de garanties supplémentaires, aucune définition précise n'en a résulté. Tout au plus a-t-on pu trouver certaines indications quant à l'interprétation à retenir de la notion[280], notamment dans le rapport explicatif de la Convention 108[281].

Selon ce texte, les données de santé couvrent « les informations concernant la santé passée, actuelle et future, physique ou mentale d'un individu ». Outre cette acception large, on constate que cette notion peut concerner un individu « bien portant, malade ou décédé », mais « également les informations relatives à l'abus d'alcool ou à la consommation de drogues ». Le groupe de l'article 29 a tenté d'adopter une approche similaire en faisant référence aux données relatives à certaines addictions ou encore aux données génétiques de la personne[282]. Prônant également une acception large de la notion de donnée personnelle de santé, ce groupe a envisagé « la définition de façon souple afin de pouvoir prendre en compte les différentes évolutions technologiques »[283]. La loi du 20 juin 2018 a consacré, préalablement à la réécriture du texte, certaines de ces recommandations en incluant notamment les données génétiques à la loi Informatique et Libertés[284].

La doctrine de la CNIL a également permis d'apporter certains éclairages quant à la définition à retenir de la notion. Elle a pu confirmer que les informations

---

[279] *Ibid.*
[280] Sophie Gambardella, « Une lecture de la jurisprudence de la Cour européenne des droits de l'Homme relative aux données de santé », *RDSS*, 2016, p. 271.
[281] Conseil de l'Europe, Rapport explicatif concernant la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Convention ouverte à la signature le 28 janvier 1981, Strasbourg, 1981.
[282] G 29, *Document de travail sur le traitement des données à caractère personnel relatives à la santé, contenues dans les dossiers médicaux électroniques (DME)*, WP 131, 15 février 2007, p. 8.
[283] Article 29 Data Protection Working Party, Advice paper on special categories of data, 4 april 2011.
[284] Article 6 (ancien art. 8) de la loi Informatique et Libertés.

relatives aux addictions, comme celles relatives au tabac, entraient dans le champ de la définition des données personnelles relatives à la santé[285] et elle a également élargi le spectre de la définition selon les cas d'espèce ; les informations relatives aux troubles mentaux ont par exemple été intégrées à la catégorie des données de santé à caractère personnel[286]. De telles précisions ont contribué à apporter certains éclairages supplémentaires quant aux informations recueillies dans le cadre de l'automesure de soi et la jurisprudence a permis, *in fine*, d'obtenir des précisions supplémentaires sur la notion.

B. L'élargissement progressif de la notion de donnée de santé

122. Souffrant d'un manque de définition légale permettant de disposer d'une définition unifiée de la donnée de santé appliquée au domaine des données personnelles, la jurisprudence est progressivement venue apporter des éclairages sur la signification de la notion **(1)**. Les arrêts rendus ne concernent pas directement le *quantified-self* mais ils mettent en lumière les besoins pratiques relatifs à l'adoption d'une définition unifiée de la donnée de santé au sein d'un texte à la force juridique contraignante. Protectrice dans son principe, l'analyse retenue se voit désormais corroborée par l'adoption du règlement européen et par la dernière modification de la loi Informatique et Libertés. Présentant une définition large, ces textes ont vocation à régir un nombre important de situations et permettent ainsi, en théorie, d'englober et de protéger une multitude d'informations issues du *quantified-self* **(2)**.

1. Le rôle protecteur de la jurisprudence

123. Les travaux préparatoires des différents textes en vigueur ainsi que la doctrine des autorités administratives indépendantes chargées de la protection des données ne donnaient à l'origine que des éclairages partiels sur le traitement des données personnelles relatives à la santé. La CJUE adoptera la première une position particulièrement protectrice envers le traitement de telles données. Celle-ci a en effet rapidement eu à se prononcer sur l'interprétation de la notion de donnée de santé,

[285] CNIL, délib. n°2013-282, 10 oct. 2013.
[286] CNIL, délib. n°2006-167, 13 juin 2006.

suivie de près par les juridictions nationales françaises et, notamment, par le Conseil d'Etat.

124. Une interprétation large. L'arrêt *Bodil Lindqvist* du 6 novembre 2003 est l'exemple le plus couramment cité en matière d'interprétation jurisprudentielle de la notion. La CJUE a ainsi précisé dans une décision à titre préjudiciel sur l'interprétation de la directive 95/46/CE que « l'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé, au sens de l'article 8, paragraphe 1, de la directive 95/46 ». La Cour s'est donc prononcée en faveur d'une interprétation large de la définition relative aux données personnelles de santé, la simple mention d'une blessure au pied étant suffisante pour retenir cette qualification[287]. Elle a en effet jugé sur ce point « qu'eu égard à l'objet de cette directive, il convient de donner à l'expression « données relatives à la santé » employée à son article 8, paragraphe 1, une interprétation large de sorte qu'elle comprenne des informations concernant tous les aspects, tant physiques que psychiques, de la santé d'une personne » [288].

Cette interprétation large de la notion a été suivie par les juridictions françaises et notamment par le Conseil d'Etat en matière de données dites administratives. Ce dernier a eu l'occasion, à plusieurs reprises, d'apporter certaines précisions concernant la définition, quitte parfois à y apporter des limites. Il considère par exemple que le fait qu'un enfant handicapé soit scolarisé dans une classe spéciale est une donnée de santé lorsque la mention « permet d'identifier immédiatement la nature de l'affection ou du handicap propre à l'élève concerné ». Il refuse pourtant de parvenir à la même conclusion lorsqu'un élève est scolarisé dans une structure de soins mais qu'il n'y a pas de précisions supplémentaires sur le type d'affection dont souffre l'élève[289]. La solution est fondée sur les possibilités de déterminer avec précision l'affection dont souffre la personne. Le simple fait de savoir que celle-ci fait l'objet de soins, en l'absence de précisions, ne permet donc pas de retenir la qualification de donnée de santé. La solution, bien que

[287] Rudolphe Munoz, « Internet et la protection des données personnelles : un élargissement du champ d'application de la directive 95/46/CE », *Communication Commerce électronique*, n°4, Avril 2004, comm. 46.
[288] CJUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003, para. 51.
[289] CE, 19 juillet 2010, n° 317182, publié au recueil. Voir aussi en ce sens : CE, 19 juillet 2010, n° 334014.

compréhensible, semble discutable car elle est susceptible de donner une indication quant à l'état de santé et laisse de plus les tiers préjuger de l'affection éventuelle.

125. L'absence de définition précise. La solution retenue par le Conseil d'Etat fait que la seule indication des mentions relatives à la structure de soins – hôpital, établissement spécialisé – sans autre indication sur la nature même des soins apportés ne relève pas du domaine des données personnelles de santé, telles qu'elles sont prévues par la loi Informatique et Libertés[290]. L'absence de précision sur la nature de l'affection ne permet pas d'intégrer les données collectées aux données relatives à la santé. Cette solution a permis d'apporter certaines précisions sur le spectre des données qui peuvent être intégrées aux données de santé mais elle n'a pas permis d'en donner une définition objective. Le RGPD, en proposant une définition élargie, est venu dissiper tout doute quant à l'acception du terme de donnée personnelle de santé.

2. Le rôle protecteur du règlement européen

126. La définition large de la donnée de santé. Le Règlement général européen sur la protection des données personnelles adopté en avril 2016 vient modifier de façon substantielle l'approche du sujet de la protection des données et notamment des données sensibles relatives à la santé[291]. Se plaçant dans la droite lignée de l'interprétation retenue par la jurisprudence européenne, le texte propose une conception large de la notion de donnée de santé visant à englober un nombre important d'informations[292].

Conformément à l'article 4 du Règlement, sont dorénavant considérées comme des données concernant la santé les « données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ». Les informations visées, en plus d'être directement listées, sont complétées par le considérant 35. Celui-ci, plus exhaustif et détaillé, apporte des

[290] AJDA 2010, p.1454, comm. M.-C. de Montecler.
[291] Jeanne Bossi Malafosse, « Le règlement européen et la protection des données de santé », *Dalloz IP/IT*, 2017, p. 260.

précisions importantes concernant la délimitation de la notion et celles-ci sont susceptibles de concerner directement le *quantified-self*. Surtout, ce considérant permet de mieux comprendre l'orientation voulue par le texte, le premier à valeur juridique contraignante à proposer une définition du terme[293].

Selon le considérant 35, « les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée […] et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro ».

127. Une définition applicable à l'automesure. Cette définition renouvelée de la notion de données de santé permet d'étendre le spectre de la protection permise par le texte. La majorité des paramètres mesurés dans le cadre d'une application de *quantified-self* sont relatives au bien-être mais les données collectées sont aussi susceptibles de « fournir des informations sur l'état de santé de l'utilisateur »[294]. Ainsi, le groupe de l'article 29 a eu l'occasion de préciser, dans le contexte de l'adoption de ce nouveau règlement, différentes interprétations des données susceptibles d'entrer dans le champ d'application de la définition. A ce titre, le spectre large des données relatives à la santé permet par exemple d'englober des informations telles que celles en rapport avec la pression sanguine, le rythme cardiaque ou encore le taux de glucose dans le sang, éléments évidemment susceptibles d'être relevés dans le cadre du *quantified-self*. Par exemple, la montre

---

[292] Estelle Brosset, « Le droit à l'épreuve de la e-santé : quelle connexion du droit de l'Union européenne ? », *RDSS*, Dalloz, 2016, p. 869.
[293] Jonathan Vayr, « Les données de santé : un enjeu pour le futur », *Petites affiches*, 16 septembre 2016, n° 185-186, p. 4.
[294] AFCDP, « Quantified-Self connecté et Informatique & Libertés », Synthèse des travaux du sous-groupe « Quantified Self » du groupe de travail « Données de santé » de l'Association Française des Correspondants aux Données Personnelles, Novembre 2015.

connectée de 4ème génération d'Apple, lorsqu'elle est connectée à une application dédiée, permet d'enregistrer un électrocardiogramme.

128. L'inclusion des données génétiques. Le règlement européen ne se limite pourtant pas au seul domaine des données de santé à proprement parler. Il définit également les données génétiques, « relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé », et les données biométriques, « résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique »[295]. Une prise en considération de ces éléments dans un texte juridique à valeur contraignante n'est pas sans incidence sur les récents développements de l'automesure connectée. On assiste ainsi depuis peu au développement d'un *quantified-self* fondé sur l'analyse du patrimoine génétique de l'individu afin de lui proposer des programmes de *coaching* adapté[296]. Un test ADN est d'abord réalisé par l'individu afin que la société proposant le service lui fournisse des conseils d'entraînement adaptés. Les dispositifs connectés de *quantified-self* pourront dès lors être utilisés, en complément, afin de suivre la progression de l'individu. Les données génétiques ainsi collectées, traitées et réutilisées par un individu ou une application sont dès lors protégées par la réglementation au titre des données sensibles.

Le spectre élargi des données de santé présenté par le RGPD permet désormais d'intégrer un nombre important de situations. Les mesures réalisées par des objets connectés et des applications peuvent tout à fait entrer dans cette catégorie. Cependant, en dehors de cette définition légale à proprement parler, le contexte de production de la donnée – données médicales provenant d'une structure de soins – permet de qualifier celle-ci et de la rattacher à une catégorie juridique précise.

[295] Article 4, Règlement (UE) 2016/679.
[296] Pour plus d'informations sur ce point, voir par exemple : https://www.genetrainer.com/

§2. Une qualification fonction du contexte de production de la donnée

129. Le *quantified-self* s'inscrit – tout en en bousculant les frontières – dans un ensemble plus vaste, relatif au bien-être mais également à la santé connectée et à la santé mobile. Les objets connectés et les applications proposées à la vente ou au téléchargement dans le cadre de l'automesure de soi ont en effet un large spectre et peuvent ainsi être utilisés dans des configurations différentes. Les données personnelles relatives à la santé ne sont donc pas uniquement qualifiées comme telles en fonction de la définition qui en est donnée par la loi Informatique et Libertés[297].

En effet, malgré des critères de définition larges, certains éléments permettent de qualifier plus précisément les données issues d'objets ou d'applications développés dans le cadre du *quantified-self*. Dans certains cas, l'origine ou le contexte dans lequel cette information est créée – clinique et hôpital par exemple – permettront de déterminer sa qualification **(A)**. Dans d'autres hypothèses, en revanche, le fait qu'une donnée puisse *in fine* révéler des éléments qui sont relatifs à la santé de l'individu entraînera sa qualification de donnée de santé **(B)**.

A. La donnée médicale *stricto-sensu*

130. Le *quantified-self* et les outils permettant sa mise en œuvre – objets connectés et applications – brouillent les frontières entre le domaine du bien-être et celui de la santé en permettant une collecte de données relative aux deux domaines[298]. Des questions relatives à la qualification peuvent dès lors survenir, mais il y a un domaine dans lequel la répartition est strictement identifiée. En effet, dans le domaine strictement médical, une donnée va recevoir la qualification de donnée de santé et donc de donnée sensible non pas en fonction de l'objet utilisé pour la collecte **(1)**, mais en raison du cadre particulier dans lequel elle est créée, ce cadre pouvant faire appel à des dispositifs de *quantified-self* **(2)**.

[297] L'article 6 de la loi renvoi à la définition donnée par le RGPD.
[298] Institut Montaigne, *Big Data et objets connectés, Faire de la France un champion de la Révolution Numérique*, avril 2015, p. 69.

1. L'indifférence de principe de l'objet utilisé pour la collecte

131. Le lien entre patient et médecin. Le *quantified-self* est généralement perçu comme une méthode d'automesure réalisée dans un cadre strictement privé et généralement ludique. Pourtant, les objets connectés ainsi que certaines applications font de plus en plus le lien aujourd'hui entre l'individu et son médecin, à tel point qu'ils peuvent désormais s'inscrire dans le cadre d'un parcours traditionnel de soins et « constituer des outils complémentaires utiles à la prise en charge des patients »[299]. Qualifiée d'ubimédecine, cette pratique repose sur une collecte quasi-permanente de données de santé par les individus qui vont les transmettre, en différents lieux et à différents moments, à des médecins ou hébergeurs de données[300].

132. Le recours aux dispositifs médicaux. Certaines sociétés spécialisées ont proposé à la vente des objets connectés et des applications permettant de collecter des données de santé, et ce sous la supervision et le contrôle d'un médecin ou d'un établissement de santé. Le tensiomètre connecté est à ce sujet un exemple topique[301]. Celui-ci permet à un individu de prendre directement sa tension artérielle chez lui et d'afficher les résultats en direct sur une application mobile. Ce dispositif connecté permet également de transmettre les données collectées au médecin, afin d'établir un suivi à distance de certaines mesures[302]. Les objets connectés relatifs à la santé brouillent dès lors les frontières classiques entre *quantified-self,* bien-être et santé mobile : les dispositifs et applications dédiées peuvent potentiellement se voir appliquer la qualification de dispositif médical.

Le régime juridique applicable aux dispositifs médicaux, largement régi par les textes européens[303], a été codifié dans l'ordre interne à l'article L. 5211-1 du Code de la santé publique qui en donne par la même occasion une définition. Selon cet article, on entend par dispositif médical « tout instrument, appareil, équipement, matière, produit, à l'exception des produits d'origine humaine, ou autre article utilisé seul ou

[299] Conseil national de l'Ordre des médecins, *Santé Connectée, De la E-santé à la santé connectée*, Le Livre Blanc du Conseil national de l'Ordre des médecins, janvier 2015, p. 6.
[300] Margo Bernelin, « La médecine connectée : interrogations et renouveau pour le droit international de la santé », *RDSS*, 2018, p. 1007.
[301] Voir par exemple le tensiomètre connecté BPM Core de la firme Withings.
[302] https://www.aphp.fr/contenu/ap-hp-deux-nouveaux-dispositifs-pour-des-patients-atteints-dhypertension-arterielle
[303] Voir notamment : directive 93/42/CEE du Conseil, du 14 juin 1993, relative aux dispositifs médicaux.

en association, y compris les accessoires et logiciels nécessaires au bon fonctionnement de celui-ci, destiné par le fabricant à être utilisé chez l'homme à des fins médicales et dont l'action principale voulue n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens ». Le champ d'application de la législation relative aux dispositifs médicaux a été récemment étendu par la directive 2007/47/CE qui a fait entrer dans la définition des dispositifs médicaux le logiciel destiné à être utilisé à des fins diagnostiques ou thérapeutiques. La qualification de dispositif médical, réalisée sous la surveillance de l'Agence nationale de sécurité du médicament et des produits de santé, entraîne son marquage « CE » avec la conséquence de « devoir satisfaire à un certain nombre de critères destinés à vérifier la qualité du dispositif »[304] au regard notamment d'exigences de sécurité et de performance[305].

133. Une qualification fonction de la finalité. La qualification de dispositif médical – objet ou logiciel – relève par ailleurs d'une casuistique, fonction de la finalité du dispositif et partant, de la volonté du fabricant[306]. Il n'est ainsi pas suffisant que le dispositif soit utilisé dans un contexte médical[307], encore faut-il que celui-ci soit destiné par son fabricant à un usage spécifiquement médical[308]. Un objet visant simplement à augmenter son activité physique, sans que son créateur lui ait attribué une quelconque finalité médicale, ne pourra recevoir la qualification de dispositif médical. Tout au plus, un tel objet pourra être présenté comme ayant un bénéfice pour la santé, au sens de l'article L. 5122-15 du Code de la santé publique. L'Agence nationale de sécurité du médicament et des produits de santé peut dès lors interdire la publicité de ceux-ci lorsqu'il n'est pas établi que lesdits objets, appareils et méthodes, possèdent les propriétés annoncées.

134. L'absence de précision sur la nature des données. Les dispositifs connectés de *quantified-self* peuvent donc tout à fait recevoir la qualification de

---

[304] Jean Bossi Malafosse, « A partir de quand peut-on qualifier un logiciel de dispositif médical ? », *Dalloz IP/IT*, 2016, p. 82.
[305] Cf., *infra*, n° 183.
[306] Paul-Anthelme Adèle, Sonia Desmoulin-Canselier, « Droit des dispositifs médicaux : vers une réforme ou un simple réaménagement ? », *RDSS*, 2016, p. 930.
[307] Décision de l'ANSM du 12 janv. 2015 portant suspension de mise sur le marché, de mise en service, d'exportation et de distribution du produit Infocament intégrant un module de compression d'images au format Waaves, fabriqué et mis sur le marché par la société CIRA, JO 10 févr. 2015.
[308] CJUE, 22 novembre 2012, *Brain Products GmbH c. BioSemi VOF*, aff. C-219/11.

dispositif médical, à condition de répondre aux exigences posées par la règlementation européenne. Pourtant, cette qualification ne donne pas forcément d'indications claires quant à la nature des données qui seront collectées par le dispositif en question. Comme le précise en effet le G29[309], la qualification de donnée de santé n'est pas tributaire de l'objet utilisé pour procéder à la collecte. Le considérant 35 du Règlement européen sur la protection des données confirme cette indifférence de principe de l'objet en indiquant qu'une donnée de santé peut être qualifiée comme telle, indépendamment de sa source, qu'elle provienne par exemple d'un dispositif médical ou d'un test de diagnostic in vitro.

Les dispositifs médicaux ont ainsi vocation à être inclus au spectre des dispositifs permettant de collecter des données de santé. Mais, indépendamment de la question de savoir si la mesure provient d'un dispositif médical, les capteurs et applications « librement disponibles sur le marché » peuvent également collecter des données de santé[310]. Une donnée peut ainsi recevoir la qualification de donnée de santé, sans prise en considération systématique de son moyen de production, confirmant ainsi qu'une donnée relative à la santé peut être issue d'un dispositif d'automesure. La qualification de donnée de santé ne dépendant pas de l'objet utilisé pour sa collecte, c'est dès lors vers le cadre de production de la donnée qu'il faudra en théorie se tourner pour déterminer avec précision et certitude la nature des données collectées.

2. Une qualification fonction du cadre de création de la donnée

135. Le groupe de l'article 29, devant la complexité à établir avec certitude une définition des données sensibles et particulièrement des données sensibles relatives à la santé a, avec l'avènement du Règlement européen sur la protection des données, rapidement tenu à identifier une catégorie particulière de données de santé. Cette catégorie de données relatives à la santé, que l'on peut qualifier de données médicales, désigne les données relatives à l'état de santé physique ou mental d'une

[309] G29, Annex – *Health data in apps and devices*, 5 février 2015.
[310] *Ibid.*

personne et qui sont recueillies dans un contexte médical par des professionnels de santé.

136. L'information obtenue dans le cadre d'une structure de soins. L'interprétation donnée par le regroupement des autorités de protection européennes permet dès lors de voir que si des hésitations peuvent apparaître entre la qualification de donnée personnelle simple ou celle de donnée de santé, c'est cette dernière qu'il faudra retenir lorsque l'information est obtenue dans le cadre d'une structure de soins. Cette solution est également celle retenue par le Conseil de l'Europe dans l'annexe à la recommandation relative à la protection des données médicales et qui considère que celles-ci ne peuvent être collectées et traitées que par des professionnels de santé[311]. Le cercle restreint des personnes pouvant traiter de telles données est lié à la nature de celles-ci : données sensibles, elles ne peuvent être collectées que par des personnes habilitées.

Le règlement européen consacre cette analyse en faisant lui-même mention des données produites dans ce cadre comme étant des données personnelles relatives à la santé. Le considérant 35 déjà mentionné inclut à ce titre « les informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ». Dans le prolongement de cette constatation, « un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé » font également partie des informations incorporées à la définition.

137. Distinguer les données créées dans un cadre médical des autres données relatives à la santé permet de mieux en délimiter le cadre et la portée. En effet, raisonner non plus à partir de la nature intrinsèque de l'information contenue dans la donnée mais à partir du cadre dans lequel celle-ci est créée, permet de passer outre la tâche souvent complexe visant à déterminer si une donnée a vocation à être qualifiée ou non de donnée de santé. Le but recherché est donc celui de pouvoir retenir la qualification de donnée de santé pour une donnée qui, dans un contexte différent,

[311] Conseil de l'Europe, Annexe à la recommandation n° R (97) 5 du Comité des ministres aux Etats-membres relative à la protection des données médicales, adoptée par le Comité des ministres le 13 février 1997, lors de la 584ème réunion des délégués des ministres.

aurait reçu une autre dénomination. Alors que dans un cas, un coureur relevant son rythme cardiaque grâce à une application mobile ne sera pas créateur d'une donnée de santé, la qualification juridique à apporter sera différente si cette mesure est réalisée par un médecin dans le cadre d'un traitement pour l'arythmie cardiaque.

138. La définition de la donnée de santé identifiée sous l'angle médical n'est pas sans rapport avec le déploiement de solutions connectées dans le cadre du *quantified-self*. Ce dernier n'est effectivement plus simplement réservé au domaine privé et peut tout à fait s'intégrer au sein d'un parcours de soin co-supervisé par un professionnel de santé[312]. Pourtant, le *quantified-self* demeure à l'heure actuelle principalement utilisé dans un cadre privé par des individus soucieux de mesurer leur bien-être, ce qui n'empêche pas de retenir la qualification de donnée de santé, mais entendue cette fois *lato sensu*.

B. La donnée de santé *lato-sensu*

139. Qu'il s'agisse de la jurisprudence nationale et européenne ou encore du nouveau Règlement européen sur la protection des données, les différents éléments composant aujourd'hui la réglementation Informatique et Libertés permettent d'affirmer que les données et outils – applications ou objets connectés – utilisés dans le cadre du *quantified-self* sont en principe pris en compte par la réglementation. A titre d'exemple, l'interprétation du G29 proposée en février 2015 concernait spécifiquement la définition des données de santé en relation avec le mode de vie et les applications de bien-être. Si l'on peut désormais constater une inclusion des données brutes collectées dans le cadre de l'automesure connectée et des conclusions relatives à l'état de santé d'une personne **(1)**, il faut voir que le principe de finalité annoncé du traitement permet, à l'image de la solution retenue pour les dispositifs médicaux, de qualifier la donnée collectée **(2)**.

[312] Melanie Swan, « The quantified-self, Fundamental Disruption in Data Science and Biological Discovery », *MS Futures Group*, Palo Alto, California, Big Data 2013, p. 85–99.

1. Données brutes et conclusions relatives à l'état de santé

140. Les conditions générales d'utilisation de certains dispositifs ou applications renseignent parfois sur la qualification à retenir des données collectées. Par exemple, les tensiomètres connectés les plus répandus sur le marché indiquent clairement collecter des données de santé[313] et il en va de même pour certains bracelets connectés ou *trackers* d'activité dont les politiques de confidentialité font une référence claire aux données de santé[314]. Les informations collectées grâce à ces outils numériques s'insèrent ainsi parfaitement dans la définition large qui est présentée par le Règlement européen.

141. Des données sans lien apparent avec la santé. Cependant, en dehors des informations directement relatives à la santé d'un individu, les objets et autres applications de l'écosystème du *quantified-self* ont vocation à relever des données qui n'ont en apparence aucun lien avec la santé : des données dites brutes ou isolées, telles que le nombre de pas parcourus ou le nombre de calories ingérées, sont donc collectées par les outils employés pour l'automesure. Le croisement de ces données, souvent insignifiantes, permet pourtant à l'individu de bénéficier de différents retours sur son activité physique ou corporelle afin d'améliorer son bien-être, ce qui est un des objectifs affirmés du *quantified-self*[315]. Mais le croisement de ces données brutes permet également d'en extraire des constantes qui sont relatives non seulement au bien-être de l'individu mais également et *in fine* à sa santé. Ainsi, les données brutes peuvent être utilisées en tant que telles mais elles peuvent également être combinées ou croisées avec d'autres données afin de tirer des conclusions sur l'état de santé ou sur les risques pour la santé d'une personne.

Cette capacité technique permise par les différents outils d'automesure connectée favorise déjà, à partir de données non-identifiantes, la révélation de données à caractère personnel. L'application de ce mécanisme au domaine de la santé a incité la Commission européenne, dès 2015, à demander au groupe de travail de l'article 29 certaines clarifications quant à la qualification des données issues

[313] https://itunes.apple.com/fr/app/ihealth-myvitals/id566815525?mt=8
[314] https://www.mykronoz.com/fr/fr/privacy-policy/
[315] Gina Neff, Dawn Nafus, *Self-Tracking*, The MIT Press Essential Knowledge series, The MIT Press, June 2016, 248 p.

d'applications et d'objets connectés relatifs au bien-être[316]. Le groupe de travail, anticipant la solution retenue par le Règlement européen concernant le caractère large de la notion de donnée de santé, a dès lors apporté certaines précisions relatives aux données qui, si elles ne révèlent pas directement des informations relatives à la santé de l'individu, sont susceptibles de donner des indications relatives à l'état de santé lorsqu'elles sont croisées.

142. Le G29 considérait alors que des données qui n'étaient pas susceptibles d'apporter des informations concernant la santé d'un individu devaient cependant être comprises comme telles à partir du moment ou combinées avec d'autres, traitées ultérieurement à d'autres fins ou encore transférées à un tiers, elles permettaient de tirer des conclusions sur l'état de santé d'une personne. Une solution similaire avait été également dégagée concernant non plus la donnée à proprement parler, mais la conclusion relative à l'état de santé de la personne elle-même. C'est non seulement la donnée brute qui doit être traitée comme une donnée de santé, mais également la conclusion tirée sur l'état de santé, peu importe que celle-ci soit juste ou pertinente.

143. Une conception large conforme au cadre européen. L'analyse adoptée par le groupe de travail de l'article 29 en 2015 est conforme à la solution finalement retenue par le Règlement européen. L'article 4 relatif aux définitions ne l'indique pas directement mais le considérant 35 précise qu'une donnée à caractère personnel concernant la santé comprend « les informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée ». Cela permet donc d'y inclure les données contribuant à tirer une conclusion sur l'état de santé d'une personne, telles que celles qui sont relevées dans le cadre de l'automesure. Dès lors, les conclusions du G29 ont permis d'apporter de nouvelles réponses sur la délimitation du spectre des données de santé issues du *quantified-self*. Ce dernier, à travers les nouveaux moyens de collecte et de traitement de données utilisés a donc une influence sur les définitions employées par la réglementation et contribue ainsi à leur évolution. Pourtant et malgré ces précisions, c'est *in fine* à la finalité pour

[316] Pour plus de précisions sur ce point, voir la réponse d'Isabelle Falque-Pierrotin à Paul Timmers, alors directeur de la Direction générale des réseaux de communication, du contenu et des technologies de la Commission européenne (DG CONNECT), consultable à cette adresse : http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf

laquelle ces données sont collectées et traitées qu'il faut faire référence pour évacuer tout doute quant à la qualification à retenir.

2. Le recours éventuel à la finalité du traitement

144. La problématique posée par le *quantified-self* réside principalement dans l'interprétation à retenir d'une information qui peut être soumise à deux qualifications juridiques, entre donnée personnelle et donnée personnelle relative à la santé. Le contexte dans lequel l'information est créée permet d'apporter des indications supplémentaires quant à la qualification à retenir. A ce titre, la CNIL a déjà eu l'occasion de faire référence à la finalité du traitement des données collectées pour déterminer avec précision la nature d'une donnée personnelle.

Ainsi, dans une délibération relative à un projet d'arrêté portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « gestion informatisée des procédures d'immigration » (GIPI), et visant à la mise en œuvre d'un fichier concernant les ressortissants étrangers contrôlés à l'occasion du franchissement de la frontière, la CNIL a eu à se prononcer sur la nature des données collectées dans le cadre d'un examen osseux visant à déterminer l'âge des personnes concernées, en l'absence de tout document d'identité[317].

145. Le critère relatif à l'objet du traitement. La CNIL, pour déterminer la qualification à retenir de la donnée issue de l'examen osseux, fait référence au critère de l'objet du traitement. Ce dernier ayant simplement vocation à déterminer l'âge des personnes concernés, elle estime que « la date et le résultat de l'examen ne constituent pas des données sensibles au sens de l'article 8 de la loi du 6 janvier 1978 modifiée ». La finalité du traitement a donc permis, dans ce cas, de déterminer la nature même de la donnée. Cette dernière n'ayant pas pour objet de déterminer l'état de santé de la personne mais seulement son âge, la qualification de donnée de santé doit être écartée, en l'absence de toute finalité sanitaire ou médicale.

[317] CNIL, délib. n°2012-431 du 6 décembre 2012 portant avis sur un projet d'arrêté portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « gestion informatisée des procédures d'immigration » (GIPI).

Le document du groupe de travail de l'article 29 relatif aux données de santé issues d'applications et de dispositifs connectés proposait une analyse similaire en faisant référence à l'usage qu'il est prévu de faire des données collectées[318]. Cette solution a également été explicitée par l'Association française des Correspondants à la protection des Données à caractère personnel qui a considéré – spécifiquement dans le cas du *quantified-self* – « qu'une même donnée pourra éventuellement être considérée comme une donnée à caractère personnel relative au « bien-être » ou comme une « donnée de santé » en fonction de son contexte d'utilisation/d'interprétation et de ses destinataires »[319].

L'AFCDP a considéré à ce titre que les données collectées grâce à une application de *quantified-self* et dont la ou les finalités visent à déduire des conclusions sur l'état de santé de la personne concernée ou des risques pour sa santé devaient être considérées comme des données de santé. L'exemple d'une donnée de fréquence cardiaque a été avancé, permettant de distinguer entre « la simple donnée personnelle recueillie par un sportif qui mesure ses propres performances et la donnée de santé recueillie par le cardiologue qui le suit en tant que patient »[320]. Ces solutions, bien qu'en apparence conformes aux utilisations qui seront faites des données, sont pourtant révélatrices des limites propres aux définitions actuellement proposées et qui sont ainsi porteuses d'insécurité juridique.

146. Conclusion du chapitre. Le cadre juridique relatif aux données personnelles, y compris aux données personnelles de santé, a fait l'objet d'évolutions progressives. Des définitions au spectre suffisamment large ont dû être adoptées pour prendre en compte les données issues d'objets connectés et d'applications de *quantified-self*. Le renouvellement des instruments juridiques employés au niveau européen a également permis d'intégrer les évolutions techniques relatives à la numérisation des activités du corps humain. Ainsi, les définitions proposées par les

[318] En anglais dans le texte : « To assess this, it does not suffice to look at the character of the data as is. Their intended use must also be taken into account, by itself, or in combination with other information » - « Pour évaluer cela [l'état de santé de la personne], il ne suffit pas de se pencher sur la nature même de la donnée. L'utilisation qui sera faite de cette donnée doit être prise en considération, seule ou en relation avec d'autres données ».
[319] Association française des Correspondants à la protection des Données à caractère personnel, *Quantified Self connecté et Informatique & Libertés*, Synthèse des travaux du sous-groupe « Quantified Self » du groupe de travail « Données de santé » de l'AFCDP, Novembre 2015, version 10.3 finale, p. 18.
[320] *Ibid.*

différents textes et les différentes interprétations qui en ont été faites devraient en théorie permettre à l'écosystème d'automesure d'être pris en compte par la réglementation. En effet, les données qui sont relevées dans le cadre de l'automesure sont identifiées et le *quantified-self*, permettant la collecte de données à caractère personnel et de données à caractère personnel sensibles éventuellement relatives à la santé, ne semble dès lors pas nécessiter la création d'une nouvelle catégorie de donnée qui lui serait propre.

Cependant, l'automesure concourt dans la pratique à la remise en question des définitions qu'elle a elle-même contribué à faire évoluer[321]. On observe ainsi une reconsidération de la distinction traditionnelle entre donnée personnelle, donnée sensible ou donnée sensible relative à la santé. Or, cet enjeu relatif à la qualification juridique des données traitées n'est pas sans conséquence : cette qualification va permettre l'application du régime juridique protecteur adéquat et contribuer, *in fine*, à la protection des droits des individus. Ainsi, l'automesure a vocation, dans certains cas, à dépasser le cadre des qualifications retenues et à en brouiller les frontières, entraînant dès lors des incertitudes quant à la nature et au régime juridique des informations traitées.

[321] Cf. *supra*, n° 142.

CHAPITRE II – LA CLASSIFICATION INCERTAINE DES DONNÉES TRAITÉES

147. Le régime juridique relatif à la protection des données à caractère personnel repose sur l'identification et la qualification préalable de telles informations. Celui-ci a donc vocation à s'appliquer dès lors qu'une opération de traitement porte sur « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres »[322]. Cette définition générale des données est complétée aux articles 6 et suivants de la loi de 1978 réécrite ainsi qu'aux articles 9 et suivants du Règlement général qui sont relatifs tous deux aux traitements portants sur des catégories particulières de données à caractère personnel. Ces dispositions permettent d'identifier une catégorie particulière de données à caractère personnel, relative aux informations identifiantes sensibles portant sur un individu. Le régime juridique applicable à cette catégorie de données met en œuvre une protection renforcée fondée sur une interdiction de principe du traitement. L'objectif de ces dispositions est de ne permettre qu'un traitement exceptionnel de données réputées sensibles et relatives à des éléments relevant de l'intimité profonde ou de la santé de la personne.

Les informations collectées par les objets connectés ne présentent en théorie pas de caractère particulier nécessitant la création d'une nouvelle catégorie de données. Identifiées par la réglementation, celles-ci sont en apparence efficacement protégées par les règles en vigueur lorsqu'elles font l'objet d'un traitement. Cette adéquation de principe du cadre juridique actuel est également confortée dans son applicabilité par les précisions apportées par la jurisprudence ainsi que par le Règlement européen sur les éléments relevant de la notion de données sensibles. Pourtant, la classification actuelle des données à caractère personnel, confrontée à la pratique de l'automesure, est susceptible d'amoindrir la portée de la protection

[322] Article 2, loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

conférée aux personnes concernées par des traitements de données. Celle-ci, reposant sur une distinction entre données à caractère personnel au sens premier du terme et données à caractère personnel sensibles, est précarisée par l'architecture même des moyens de collecte et de traitement mis en œuvre dans le cadre du *quantified-self*.

148. Une confusion sur la nature des données collectées. La pratique du *quantified-self* a en effet pour particularité de procéder à une collecte étendue de données complémentaires et de nature différente. Or, la corrélation de ces différentes informations et la routinisation des opérations de collecte a tendance à remettre en cause la distinction établie entre données personnelles classiques et données sensibles. En effet, des données ne présentant pas de caractère sensible lors de leur création sont susceptibles, par accumulation, de révéler des éléments relevant de la qualification et du régime juridique des données sensibles. Cette capacité d'interconnexion de données n'est, à l'heure actuelle, que partiellement prise en compte par la réglementation. Surtout, celle-ci ne fait aucune référence à la notion de « bien-être », finalité première de la pratique de l'automesure. Ainsi, en dehors du volume, du croisement ou de l'interconnexion, ces données dépassent dans certains cas, par leur caractère protéiforme et leur nature ambivalente, la distinction établie par la réglementation.

Une application servant à compter le nombre de calories ingérées chaque jour par une personne pourra ainsi permettre le recueil de deux types de données : donnée à caractère personnel simple dans le cas d'un individu suivant un régime ou donnée à caractère personnel sensible lorsqu'une telle application sert à surveiller l'état de santé d'un individu en surpoids. La question de la qualification de la donnée est posée au regard notamment du contexte de création de la donnée, entre amélioration du bien-être dans un cas et surveillance de l'état de santé dans l'autre. Pourtant, l'information relevée dans ces deux contextes, bien qu'identique, sera éventuellement soumise à des régimes juridiques distincts et à des degrés de protection différents.

149. Une confusion sur la nature des dispositifs employés. Le développement progressif d'un véritable écosystème de santé connectée est également à même de précariser le cadre juridique applicable. Les rapports entre *e-health* (santé connectée), *m-health* (santé mobile), *quantified-self* et télémédecine sont de nature à

semer le doute sur les rapports entre les activités opérées dans ces différents cadres et leurs implications au regard de l'ensemble de la réglementation relative à l'informatique et aux libertés. Ces différents éléments, souvent complémentaires mais également utilisés de manière autonome, permettent la création d'un nombre important de données, utilisés dans des cadres et pour des finalités différentes.

150. Par ailleurs, le cadre juridique particulier auquel sont soumis les dispositifs médicaux connectés, dont les caractéristiques se rapprochent souvent des objets connectés destinés au grand public et utilisés dans le cadre du *quantified-self*, est également de nature à ajouter une couche de complexité supplémentaire à la protection des données à caractère personnel sensibles. Cette complexité croissante des éléments relatifs à la santé connectée, ainsi que leurs implications au regard du *quantified-self*, permet de révéler la frontière poreuse qui existe entre données personnelles et données de santé **(section 1)**, tout en montrant les insuffisances du recours au principe de finalité dans la mise en œuvre de cette distinction **(section 2)**.

SECTION I – LA FRONTIÈRE POREUSE ENTRE DONNÉES PERSONNELLES ET DONNÉES DE SANTE

151. La pratique de l'automesure, par les rapports qu'elle peut entretenir avec d'autres dispositifs de santé connectée, fragilise le cadre juridique applicable aux traitements de données. En l'absence d'éléments clairs permettant de trancher d'éventuels conflits de qualification, certaines données pourraient être insuffisamment protégées, contribuant au risque informationnel pesant sur les individus. A l'inverse, des données non-sensibles relevant du régime général de protection pourraient faire l'objet de mesures protectrices injustifiées. Or cette protection *a maxima* d'informations courantes pourrait potentiellement freiner les capacités d'innovation de certains services par la mise en œuvre d'un régime juridique trop contraignant.

Entre limitation de la protection pour l'individu d'un côté et limitation de l'innovation et des bénéfices pour la santé de l'autre, les hésitations sur la qualification juridique à retenir peuvent potentiellement amoindrir la protection des données collectées dans le cadre du *quantified-self* **(Paragraphe 1)**. Cette protection peut également être limitée par la problématique multi-échelle propre au fonctionnement du *quantified-self* **(Paragraphe 2)**.

§1. La protection à géométrie variable des données d'automesure connectée

152. Le développement du *quantified-self* permet de mettre en lumière les limites de la distinction en vigueur à l'heure actuelle entre données personnelles à caractère sensible ou non. Les objets connectés et applications mobiles, produits à l'origine de grande distribution et ayant vocation à être utilisés dans un cadre ludique, ont rapidement eu tendance à proposer des services de plus en plus performants, précis et spécialisés. En s'immiscent progressivement dans le domaine de la santé, la connexion d'objets du quotidien à Internet a permis un recueil de données touchant progressivement à l'intime et au corps humain. Destinée à l'origine à mesurer

l'activité physique, l'automesure connectée contribue de manière plus générale à quantifier le bien-être de l'individu. L'inexistence juridique de cette notion appliquée aux données à caractère personnelles **(A)** est révélatrice de l'ambivalence des données qui ont vocation à être collectées **(B)**.

A. L'inexistence juridique de la notion de donnée de bien-être

153. La recherche du bien-être est au cœur même du développement du *quantified-self* et du déploiement de solutions toujours plus innovantes dans ce cadre. Le bien-être doit pourtant être distinguée, juridiquement, de la notion de santé qui est prise en compte par la réglementation. En effet, le bien-être n'est à l'heure actuelle pas inclus au sein de la réglementation relative à la protection des données personnelles, qu'il s'agisse de la loi de 1978 modifiée ou du Règlement général européen. La thématique du bien-être connaît pourtant un développement certain dans notre société et fait l'objet d'une prise en compte progressive par les politiques publiques et par le droit, visant ainsi à favoriser l'épanouissement des personnes. Relativement nouvelle **(1)**, cette notion reste également largement imprécise **(2)**.

1. Une notion nouvelle

154. Le dictionnaire Larousse définit le bien-être comme un « état agréable résultat de la satisfaction des besoins du corps et du calme de l'esprit »[323]. Matérialisée par le fait que les individus doivent prendre soin d'eux tout au long de leur vie, la notion de bien-être ne se trouve plus seulement dans les campagnes de santé publique. Celle-ci est également présente dans des lois plus générales telles que celles en faveur des personnes handicapées, ou contre les discriminations, mais aussi dans des lois relatives à l'égalité entre hommes et femmes ou aux droits de l'enfant[324]. Par ailleurs, l'application de la notion de bien-être à la condition animale a encouragé sa consécration juridique[325].

[323] https://www.larousse.fr/dictionnaires/francais/bien-%C3%AAtre/9159
[324] Martial Meziani, « Le bien-être : enjeux relatifs aux droits et approche pluridisciplinaire », *JS*, 2015, n°151, p. 18.
[325] Muriel Falaise, « Bien-être animal et abattage : la nouvelle donne européenne », *Revue de l'Union Européenne*, 2012, p. 331.

La détermination objective du bien-être se montre parfois difficile à établir. Mais elle permet de justifier la place qui est désormais faite aux dispositifs d'auto-évaluation. Les applications pour *smartphones* destinées à l'automesure du niveau de performance pendant l'activité physique répondent ainsi « à une demande sociale visant à mesurer cette performance, afin d'obtenir un *satisfecit* non seulement pendant la durée de l'exercice, mais aussi dans le cadre d'un programme de remise en forme »[326]. La pratique du *quantified-self* s'inscrit dans le prolongement de ce paradigme. Il ne s'agit dès lors pas de procéder à une évaluation subjective du bonheur, mais à une quantification objective des progrès réalisés dans le but d'atteindre un certain bien-être. Les applications de *quantified-self* contribuent ainsi à déterminer des paliers à atteindre et prodiguent des conseils permettant de réaliser ces objectifs. L'application de *running* Nike+ Run Club permet par exemple de créer des programmes personnalisés de course à pieds avec des objectifs de temps et de distance à réaliser chaque semaine.

155. Une nouvelle relation au corps. La multiplication des bracelets connectés et des dispositifs d'automesure ne concerne plus seulement la mesure de la performance ; elle s'inscrit plus globalement dans une nouvelle relation au corps pour l'individu. Ce dernier, avant de pouvoir observer en continu les effets de son activité physique grâce à des dispositifs nouveaux, « devait s'en remettre à des instruments extérieurs à son corps comme le chronomètre ou au jugement de son entraîneur au bord de la piste ou du bassin »[327]. La pratique du *quantified-self* permet désormais de mesurer objectivement la quotité de bien-être ressenti, modifiant également le rapport au corps humain. Le culte du corps « et la passion de bien-être sont ainsi devenus un mode de subjectivation par lequel le sujet se construit et par lequel il est aussi gouverné »[328]. Or, cette gouvernance nouvelle est rendue possible par l'analyse de données à caractère personnel relatives au bien-être de l'individu et qui vont aider à la prise de décision et à l'adoption de nouveaux comportements.

[326] Gilles Ferréol, « Qu'entend-on par bien-être ? Un éclairage socio-économique », *JS*, 2015, n°151, p. 31.
[327] Bernard Andrieu, « Traquer son bien-être et propriété des données : quel droit des sportifs 3.0 sur leur corps vivant ? », *JS*, 2016, n°162, p. 36.
[328] Gilles Raveneau, « Des sports à la jonction de la passion du bien-être et du culte du corps », *JS*, 2015, n°151, p. 25.

2. Une notion imprécise

156. La remise en question de la frontière entre bien-être et santé. Une confusion existe aujourd'hui entre les notions de bien-être et de santé. Celle-ci est renforcée par la définition de la santé qui est donnée par l'OMS ainsi que par les nouveaux modes de collecte et de traitement de données, tels que les objets connectés[329]. La nature des données issues du *quantified-self* interroge et la question se pose de savoir si les bracelets connectés sportifs comptant les pas effectués dans une journée, calculant les calories brûlées et analysant la qualité de sommeil d'un individu collectent des données de santé[330]. Pourtant, si l'on en revient à la définition de la santé telle qu'elle est donnée par l'OMS, « celle-ci ne signifie pas que santé et bien-être sont synonymes, mais plutôt que la première, notamment par ses aspects physiques, mentaux et sociaux, importe pour se sentir bien, et donc pour avoir un certain bien-être »[331]. Dès lors, en suivant ce raisonnement, les données relatives au bien-être pourraient être intégrées aux données relatives à la santé et donc aux données sensibles puisqu'elles n'en constitueraient qu'une émanation. Le *quantified-self*, outil de mesure du bien-être, s'insèrerait ainsi de manière plus générale parmi des instruments de mesure relatif à la quantification de la santé de l'individu.

Les frontières entre le domaine du bien-être et celui de la santé sont donc théoriquement minces. Pourtant, le cadre juridique actuel ne prend pas en compte cette distinction et « pose des incertitudes quant au régime qu'il convient d'appliquer à ce type de données » [332]. L'application d'un régime juridique inadapté aux données collectées présente en effet l'inconvénient de ne pas pouvoir permettre une prise en compte de toutes les subtilités relatives à de telles informations et empêche par ailleurs toute éventualité de gradation de la protection à apporter. Outre les écarts de protection qu'elle est susceptible d'apporter, cette absence de prise en compte de la donnée de bien-être, confirmée par l'adoption d'une définition large des données de santé par le RGPD, est renforcée par la problématique de l'interconnexion de

[329] Elise Debiès, « L'ouverture et la réutilisation des données de santé : panorama et enjeux », *RDSS*, 2016, p. 697.
[330] Gérard Haas, Amanda Dubarry, Marie D'Auvergne, Rachel Ruimy, « Enjeux et réalités juridiques des Objets Connectés », *Dalloz IP/IT*, 2016, p. 394.
[331] Anne Laude, « Le bien-être et le malade », *in* Marta Torre-Schaub (dir.), *Le bien-être et le droit*, Paris, Publications de la Sorbonne, 2016, p. 78.
[332] *Ibid.*

données. Des données à caractère personnel, en apparence non-sensibles et donc protégées à ce titre, peuvent le devenir en raison des capacités de croisement, d'analyse et de déduction mises en œuvre par les outils utilisés pour la pratique du *quantified-self*.

B. Des données de nature ambivalente

157. Le *quantified-self* permet la création de données à caractère personnel qui sont relatives au bien-être de l'individu. Cette notion ne permet pourtant pas de classer les données dans une des catégories établies par la réglementation relative à la protection des données personnelles. Les données collectées par les objets et applications, ayant vocation à s'insérer dans une des deux catégories existantes, en repoussent cependant les limites du fait de leur ambiguïté. Des données qui ne sont pas sensibles ou révélatrices de l'état de santé pourraient, en raison du caractère particulièrement intime des informations en cause, nécessiter une protection renforcée selon une distinction qui est aujourd'hui absente du cadre juridique. Aux doutes relatifs à l'inexistence juridique de la notion de donnée de bien-être s'ajoutent ceux relatifs aux modalités d'interconnexion de données en apparence non-sensibles **(1)** et à l'absence de cohérence des politiques de confidentialité **(2)**.

1. L'interconnexion de données non-sensibles

158. L'essor du *big data*. Les capacités de croisements des données collectées dans le cadre du *quantified-self* sont susceptibles de renouveler les interrogations relatives à la qualification des données à caractère personnel qui en sont issues. Les objets connectés et applications peuvent relever différents types de mesures pouvant, à l'heure des *big data*, être croisées avec des données provenant d'autres sources et permettant de multiplier les informations relatives à un seul individu.

La constitution et l'exploitation de grandes masses de données dans le but de les transformer en informations renvoie ici à « l'ensemble de technologies et de méthodes consistant à analyser, à des fins généralement prédictives, le flot de données produites par les entreprises, les organisations et les individus, mais aussi les

objets s'ils sont connectés, dans des volumes et à une vitesse sans précédent »[333]. Or, au gré des corrélations de données effectuées, la qualification appliquée aux données sera susceptible d'évoluer dans l'un ou l'autre des deux sens, faisant dès lors varier l'intensité de la protection accordée à de telles informations.

159. L'essor des capacités de corrélation. La démultiplication des masses de données produites grâce aux progrès techniques et au développement de nouveaux usages constitue une première difficulté. Une seconde difficulté apparaît également, liée à « l'essor des capacités de traitement dont les coûts sont en constante diminution, essor qui permet de collecter et d'exploiter ces masses de données en temps quasi réel »[334]. Ce sont dès lors les capacités de corrélation qui sont susceptibles de révéler des données relevant en théorie du champ des données sensibles. Une donnée relative à la foulée d'un individu ne donnera en théorie aucune indication sur la santé de celui-ci. Mais son évolution dans le temps, associée à des informations relatives au poids, au rythme cardiaque ou à un régime alimentaire particulier, sera *in fine* susceptible de révéler des informations concernant l'état de santé. Le risque du développement du *quantified-self* en matière de santé serait justement de permettre aux responsables de traitement de s'affranchir des contraintes légales, réglementaires et déontologiques et de venir concurrencer « l'offre numérique régulée »[335].

Cette interconnexion de données d'apparence non-sensibles a également été identifiée par le G29 dans son avis relatif aux récentes évolutions de l'Internet des objets. Celui-ci indique qu'il est possible « en observant les tendances et les changements de comportement au fil du temps […] d'analyser les données collectées afin d'en déduire des informations qualitatives relatives à la santé, y compris des appréciations sur la qualité et les effets de l'activité physique, basées sur des seuils prédéfinis et la présence probable de symptômes de maladie »[336]. Suivant le document

[333] Alexandra Bensamoun, Célia Zolynski, « Big data et privacy : comment concilier nouveaux modèles d'affaires et droits des utilisateurs », *Les Petites Affiches*, 18 août 2014, n° 164, p. 8.
[334] *Ibid*.
[335] Clémentine Lequillerier, « L'« ubérisation » de la santé », *Dalloz IP/IT*, 2017, p. 155.
[336] G 29, *Avis 8/2014 sur les récentes évolutions relatives à l'internet des objets*, 1471/14/FR WP 223, adopté le 16 septembre 2014.

du G29, il serait donc possible de retenir différents types de données : données brutes, données agrégées, informations extraites et données affichables[337].

160. L'absence de critères précis de distinction. Le groupe de l'article 29 a déjà proposé la notion de conclusions relatives à l'état de santé[338] pour prendre en compte les données qui, par corrélation, permettent de déduire des informations relatives à la santé de l'individu. Pourtant, cette distinction entre donnée brute et donnée analysée résultant d'une corrélation de données brutes ou d'une production algorithmique n'apporte pas de réponse définitive. D'abord, « l'opacité des écosystèmes entourant les objets connectés en matière de santé et les applications mobiles les accompagnant ne sont […] guère faits pour rassurer des consommateurs qui peuvent légitimement se demander quels acteurs ont accès à des informations particulièrement sensibles, mais aussi quelles mesures de sécurité sont mises en œuvre »[339]. Ensuite, la notion de conclusions relatives à l'état de santé dégagée par le G29 fait que toute donnée collectée dans le cadre du *quantified-self* aurait vocation à devenir donnée sensible, en raison des capacités d'interconnexion de telles données. L'absence de cohérence des politiques de confidentialité des différents opérateurs appelés à collecter des données renforce cette possibilité et augmente ainsi le risque d'éclatement de la protection des données et de la pulvérisation des droits dont l'individu est censé bénéficier.

2. L'absence de cohérence des politiques de confidentialité

161. La pertinence des mesures réalisées dans le cadre du *quantified-self* repose, dans certains cas, sur la collaboration de différents opérateurs dans la collecte et l'analyse des données. La diversité des opérations réalisées sur une donnée par des acteurs différents nécessite dès lors une multiplication des transferts. Or, des divergences entre les politiques de confidentialité mises en œuvre sont susceptible d'accroître le risque informationnel pesant sur les individus. Un opérateur va définir dans ses propres conditions générales d'utilisation les modalités selon lesquelles il traitera des données à caractère personnel. Mais un autre opérateur, appelé à traiter

[337] *Ibid.*, p. 7.
[338] Cf., *supra*, n° 142.

également les données, pourrait être enclin à mettre en œuvre une politique de confidentialité différente et éventuellement moins respectueuse des informations relatives à l'individu.

Le manque de précision des finalités annoncées conduit dans certains cas à ne pas pouvoir fournir à l'individu une pleine information de l'utilisation et de la réutilisation dont les données collectées peuvent faire l'objet. La politique de confidentialité de l'application *Runkeeper*, application de *running* visant à mesurer l'effort physique fourni, indiquait antérieurement à l'adoption du RGPD que « si vous transmettez des données personnelles pour une certaine raison, nous sommes susceptibles d'utiliser vos données personnelles pour la raison pour laquelle vous nous les avez transmises »[340]. Modifiées postérieurement à l'entrée en application du RGPD, cette politique de confidentialité indique désormais que les données sont collectées « pour l'exécution de l'accord que nous avons passé avec vous »[341]. Outre le caractère vague de ce type de politique de confidentialité, l'absence de cohérence entre celles-ci contribue au renforcement du risque informationnel. Les individus ne seront pas *in fine* en mesure de déterminer avec précision la nature, sensible ou non, des données traitées ainsi que les éventuelles utilisations qui pourront en être faites.

162. Le recours à des tiers. Dans certaines hypothèses, le responsable de traitement aura recours à des tiers qui seront théoriquement liés par le principe de finalité initialement instauré, conformément à l'article 5 du RGPD qui indique que les données ne sont pas traitées d'une manière incompatible avec celle-ci. Le consentement qui est donné pour un traitement devrait dès lors valoir, conformément au considérant 32 du RGPD, pour toutes les activités de traitement ayant la ou les mêmes finalités. Par ailleurs, la précision des règles entourant le mécanisme de la sous-traitance empêche, lorsqu'il est fait recours à un sous-traitant, que ce dernier ne puisse traiter les données pour des finalités différentes que celles établies par le responsable de traitement. Mais les modalités d'utilisation des données par les tiers

[339] Isabelle Falque-Pierrotin, « La CNIL face à l'économie de la donnée », *AJCA*, 2016, p.175.
[340] En anglais, dans le texte : « If you provide Personal Data for a certain reason, we may use the Personal Data in connection with the reason for which it was provided ».
[341] https://www.asics.com/privacy/privacy/fr-fr/privacy-french.html

potentiellement impliqués soulèvent d'autres interrogations, notamment pour les cas où le tiers n'est pas directement placé sous la supervision du responsable de traitement principal, en vertu d'un contrat de sous-traitance[342]. A titre d'exemple, les conditions générales d'utilisation de l'application de remise en forme *My Fitness Pal* indiquent :

> *« la présente Politique de confidentialité ne s'applique pas aux pratiques des sociétés qui ne nous appartiennent pas ou sur lesquelles nous n'exerçons aucun contrôle ni aux personnes qui ne sont pas nos employés ou ne relèvent pas de notre responsabilité. Par exemple, si vous téléchargez une de nos applications sur votre smartphone, il est possible que le fabricant de votre smartphone ait mis en place une politique qui s'applique à ses pratiques de collecte de données par le biais de cet appareil. Nous vous recommandons de lire les politiques de confidentialité de tout appareil, site Internet et services que vous utilisez »*[343].

Dans ce cas de figure, le responsable de traitement sera obligé de recourir à des prestataires pour qui les modalités contraignantes de mise en œuvre d'un traitement n'auront pas forcément vocation à s'appliquer de la même manière : une application d'automesure sera par exemple et dans certains cas, dépendante du média sur lequel elle est installée, *smartphone* ou tablette. Cependant, bien qu'ils ne soient pas liés aux responsables de traitement initiaux, les développeurs de ces différents médias sont responsables des données à caractère personnel qu'ils collectent et doivent mettre en œuvre des politiques de confidentialité, déterminer une finalité et se conformer aux principes de la réglementation relative à la protection des données.

163. Le partage sur les réseaux sociaux. La pratique de l'automesure contribue à l'amplification des modalités d'exposition de soi qui sont permises par de plus en plus de services numériques. Les réseaux sociaux permettent à ce titre aux

---

[342] Dans ce cas de figure précis, les conditions générales d'utilisation de l'application *My Fitness Pal* indiquent qu'en vertu « du principe de transfert ultérieur, le traitement des Données personnelles européennes que nous transférons à nos agents ou prestataires de services tiers est susceptible de relever de notre responsabilité ».

[343] *My Fitness Pal*, conditions générales d'utilisation, disponibles en ligne à cette adresse : https://account.underarmour.com/fr-fr/privacy

utilisateurs de partager, dans certains cas, les résultats issus de l'utilisation d'objets connectés à leurs contacts ou « ami(e)s » sur de tels réseaux. Or, comme l'indiquent directement certains responsables de traitement, « dans le cas où l'utilisateur choisit de partager ses Données Personnelles sur les réseaux sociaux, ce partage se fait conformément aux conditions d'utilisation du réseau social utilisé et à la politique de confidentialité propre à ce réseau social »[344]. En l'absence de tout accord éventuel sur le partage de données entre le responsable de traitement initial et le réseau social, notamment quant aux finalités du traitement, l'individu souhaitant partager ses données sur un tel réseau le fera conformément à l'engagement de confidentialité du réseau social concerné. Les données de santé collectées sont dès lors susceptibles d'être partagées selon une « extériorisation de l'intimité » qui s'est installée avec une « facebookisation des données de santé »[345].

164. Outre des finalités de traitement différentes, les modalités selon lequel les réseau sociaux sont susceptibles de traiter les données partagées sont potentiellement différentes de celles annoncées en amont par le responsable de traitement initial, fournisseur du service de *quantified-self*. L'utilisateur est ici à l'origine du partage de ses propres données vers un service tiers, mais les finalités pour lesquelles les données ont été collectées à l'origine sont altérées par ce partage et renforcent le risque informationnel pesant sur l'individu. Surtout, les données collectées par le premier responsable de traitements seront assimilables à des données non-sensibles. Mais, le partage de ces données à un autre responsable de traitement rendra *in fine* possible le croisement de celles-ci avec d'autres informations, permettant de révéler des éléments relatifs à la santé de l'individu.

§2. La problématique multi-échelle du quantified-self

165. Le développement de services d'automesure connectée correspond à l'apparition de nouveaux acteurs se présentant le plus souvent comme des plateformes. Les moyens humains, financiers et techniques dont disposent

[344] Voir à ce titre les conditions générales d'utilisation de la société *iHealth*, fabricant d'objets connectés et fournisseurs d'applications, disponibles en ligne à cette adresse : https://ihealthlabs.eu/fr/content/186-notice-de-donnees-de-sante
[345] CNIL, *Le corps, nouvel objet connecté ?*, *op. cit.*, p. 14.

aujourd'hui ces entreprises permettent effectivement le renforcement de leurs capacités d'analyse et celles-ci renforcent le risque informationnel qui pèse sur les individus. En effet, le modèle économique suivi par ces plateformes s'oppose à certains principes de la réglementation. Ces derniers, mobilisés pour apprécier la licéité de la collecte et du traitement réalisé, peuvent également servir à déterminer la nature et la qualification juridique des données traitées.

Le regroupement des moyens de collecte au sein de plateformes, corroboré par une collecte exponentielle de données à caractère personnel des individus, renforce les hésitations sur la qualification juridique à apporter aux données traitées. Un double constat s'impose : la concentration de la surveillance qui est mise en œuvre à l'égard des individus a vocation à favoriser la qualification de donnée sensible **(A)** et doit conduire à l'adoption de mesures correctrices **(B)**.

A. Une concentration de la surveillance

166. La pratique de l'automesure, susceptible de révéler l'état de santé d'une personne, révèle l'irruption d'une surveillance opérée hors les cadres traditionnels de la médecine. Fondée sur l'analyse des grands ensembles de données ou *big data*, cette surveillance à la fois du bien-être et d'éléments relatifs à la santé repose sur l'utilisation d'outils de calcul permettant la corrélation d'informations issues de sources diverses. Le propre de l'automesure est ainsi de pouvoir utiliser différents outils de collecte et de traitement pouvant dialoguer entre eux dans le cadre de l'Internet des objets. Or, les modalités de croisement et d'analyse des données permettent de révéler non seulement le rôle qui est tenu par les algorithmes dans l'interprétation des données relevées **(1)**, mais favorisent également la concentration de celles-ci aux mains d'acteurs nouveaux **(2)**.

1. Le rôle des algorithmes dans l'interprétation des données

167. Selon la CNIL, « un algorithme est la description d'une suite finie et non ambigüe d'étapes (ou d'instructions) permettant d'obtenir un résultat à partir

d'éléments fournis en entrée »[346]. Dès lors, ces algorithmes rendent possibles la combinaison d'informations de natures et de sources variées pour produire différents résultats. Exprimé dans un « langage informatique, transcrit en un programme (une sorte de texte composé de commandes écrites, également appelé « code source »), ce programme peut alors être exécuté dans un logiciel ou compilé sous la forme d'une application »[347]. Déjà identifiés et définis par la jurisprudence nationale[348], ces algorithmes poursuivent différents buts, tels que « produire des connaissances ; apparier une demande et une offre ; recommander un produit ou une offre de façon personnalisée ; aider la prise de décision ; prédire, anticiper »[349].

168. Les algorithmes prédictifs. Les algorithmes prédictifs, catégorie spécifique d'algorithmes, jouent un rôle particulier en matière d'automesure connectée. D'une part, ils peuvent aider l'individu à déterminer des objectifs à atteindre lors d'activités physiques. D'autre part, ils contribuent à la patrimonialisation des données à caractère personnel des individus. En effet, les responsables de traitement peuvent avoir recours à des algorithmes prédictifs pour personnaliser leurs offres commerciales, en fonction des préférences, des habitudes de navigation ou de la géolocalisation. Les algorithmes permettent ainsi d'établir des profils comportementaux des individus dans le but d'anticiper leurs attentes. Mais ils contribuent également, par leur mode de fonctionnement, à transformer des informations en données sensibles. En effet, l'appariement de différentes données personnelles par le biais d'algorithmes permet dans certains cas d'inférer ou de créer des données sensibles, relatives, dans certains cas, au bien-être et à la santé.

La collecte de données à caractère personnel constitue le préalable à l'automesure et sa numérisation par les objets connectés est l'élément permettant son automatisation. Certaines des données relevées dans le cadre de l'automesure offrent, en elles-mêmes une information exploitable. D'autres, en revanche, « prennent toute

[346] CNIL, *Comment permettre à l'homme de garder la main ?,* Les enjeux éthiques des algorithmes et de l'intelligence artificielle, 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, décembre 2017, p. 15.
[347] *Ibid.*
[348] Voir par exemple : Cour d'Appel de Paris, 23 juillet 1995, qui qualifie un algorithme de « succession d'opérations mathématiques traduisant un énoncé logique de fonctionnalités ».
[349] CNIL, *op. cit.*, p. 20.

leur valeur en étant couplées, assemblées, recoupées, grâce aux algorithmes »[350]. La plus-value de l'automesure, lorsqu'elle est connectée, repose donc sur ces modalités d'interconnexions de données permettant d'accéder à une analyse toujours plus poussée des mesures relevées. Conférant ainsi une véritable valeur aux données qui sont traitée, le recours aux algorithmes explique l'appétence des responsables de traitement et fournisseurs de services, non seulement pour les données à caractère personnel, mais également pour les traces numériques laissées par les individus lors de l'utilisation des services.

169. Ainsi, les algorithmes apparaissent comme l'outil privilégié permettant de donner un sens à l'ensemble de données collectées dans le cadre du *big data*. Cette hypothèse est particulièrement vraie en matière prédictive : les algorithmes permettent d'affiner les résultats proposés en amont aux individus. Or, comme le montrent certains auteurs, « les données utiles aux algorithmes prédictifs sont disparates, évolutives et sans valeur intrinsèque » et sont en outre, « subjectives, comportementales et décontextualisées »[351]. La réglementation relative à la protection des données à caractère personnel ne serait dès lors pas susceptible d'appréhender efficacement les mécanismes de traitement mis en œuvre par les algorithmes, étant donné que ceux-ci sont susceptibles de conduire à une modification de la nature des informations traitées.

La notion de traitement étant entendue comme « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés » [352], les modalités de calcul mises en œuvre par les algorithmes entrent dans le champ d'application de la LIL et du RGPD. Mais de telles opérations doivent porter sur des données à caractère personnel. Or, bien que cette définition soit comprise de manière large, le dispositif mis en œuvre est susceptible d'exclure de la protection certaines opérations réalisées à partir de données non-identifiantes mais tout autant révélatrices de l'intimité des individus.

[350] Maryline Boizard, « La valorisation des données numériques par la protection juridique des algorithmes », *Dalloz IP/IT*, 2018, p. 99.
[351] Lêmy D. Godefroy, « Pour un droit du traitement des données par les algorithmes prédictifs dans le commerce électronique », *Recueil Dalloz*, 2016, p. 438.
[352] Article 4, Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

170. A l'heure actuelle, seule la référence à la notion de profilage semble permettre une prise en compte des traitements réalisés par algorithme. En effet, cette « ubiquité algorithmique »[353], mise en œuvre par les objets connectés et applications dans le cadre du *quantified-self*, sert justement à « évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire », selon la définition de l'article 4 du Règlement général européen. L'article 22 du texte fait référence à la production d'effets juridiques de cette opération et le considérant 24 précise que celle-ci peut avoir pour objet d'analyser ou de prédire des préférences, des comportements et des dispositions d'esprit. Dès lors, la personne concernée par ce type d'opérations devrait être informée non seulement de l'existence d'un profilage mais également des conséquences de celui-ci. Notamment, pour les cas de prospection, la personne concernée par un tel traitement devrait pouvoir s'y opposer, qu'il s'agisse d'un traitement initial mais également d'un traitement ultérieur qui recouvrirait les éventuelles réutilisations de données. Cette faculté d'opposition de l'individu est aujourd'hui limitée par le caractère vague des conditions générales d'utilisation dans lesquelles sont situées ces mentions.

La notion de profilage telle qu'elle est entendue par le Règlement européen mentionne expressément la santé au titre des éléments pouvant faire l'objet d'analyses ou de prédictions. Or le *quantified-self*, par la diversité des mesures interprétées et la multiplication des sources de données, est justement susceptible de dresser des profils relatifs à la santé de l'individu par le truchement d'algorithmes. Dès lors, toute information pourrait « devenir donnée sensible, en fonction des jeux de données recoupées et de l'utilisation finale qui en ressort », car si ce ne sont pas les données qui, prises individuellement, sont susceptibles de révéler des informations relatives à l'état de santé, « la vraie révélation vient de l'accumulation d'informations et des nouvelles techniques d'analyse algorithmique des données »[354]. Dès lors, la protection devrait avoir pour objet, non seulement le traitement algorithmique en tant que tel, mais surtout le résultat produit par un traitement algorithmique, nouvelle donnée sensible relative à un individu. La répétition de mesures de la fréquence

[353] Jean-Baptiste Duclercq, « Le droit public à l'ère des algorithmes », *Revue du Droit public*, octobre 2017, n°5, p. 1401.
[354] Renaissance Numérique, *D'un système de santé curatif à un modèle préventif grâce aux outils numériques*, 16 propositions pour un changement de paradigme des politiques de santé, septembre 2014, p. 35.

cardiaque opérées par un coureur pourra par exemple, grâce à l'aide d'une application spécialisée, révéler l'apparition de troubles cardiaques. Dans ce cas, la protection à apporter devrait concerner les différentes mesures réalisées mais également la conclusion relative à la dégradation de l'état de santé.

171. La course aux données de santé. Les capacités renforcées de calcul algorithmiques sont en majorité déployées par un nombre restreint de sociétés du numérique, en raison de leurs moyens financiers importants et du budget qu'elles allouent à la recherche. La course aux données de santé[355] à laquelle ces sociétés du numérique prennent part grâce à leurs capacités de collecte et de traitement, en font les dépositaires et gestionnaires d'une quantité considérable de données. Celles-ci, souvent sensibles, par nature ou par suite de leur traitement, sont donc concentrées entre les mains d'acteurs nouveaux opérant dans le domaine de la santé.

2. Une concentration de données sensibles aux mains d'acteurs nouveaux

172. La création de données sensibles par le recours au *quantified-self* et aux objets connectés a pour effet de doter les entreprises du numérique d'une masse importante d'informations relatives à la santé. A ce titre, « la massification dans la collecte des données et les capacités de traitement rapide de ces dernières […] confortent l'idée que l'économie numérique favorise le développement d'acteurs dominants dont les positions sont quasi incontestables »[356]. Outre des questions posées en matière de droit de la concurrence et d'éventuels abus de position dominante, celle du regroupement de données par le même opérateur est particulièrement susceptible de nuire aux droits des individus.

En effet, cette concentration de données sensibles entre les mains d'acteurs du numérique a surtout pour conséquence de faire sortir des cadres institutionnels nationaux un grand nombre d'informations qui, si elles peuvent avoir une utilité publique, sont également et théoriquement protégées par des personnes publiques. En effet, les entreprises proposant des services de *quantified-self*, si elles deviennent de

[355] Conseil d'Etat, *op. cit.*, p. 62.

fait dépositaires de données de santé, ne présentent pas les mêmes garanties au regard des modalités d'accès, de transmission, de diffusion ou de réutilisation que celles mises en œuvre par les administrations au regard des bases de données sanitaires dont elles organisent la gestion.

173. Une surveillance par des acteurs publics. La surveillance sanitaire est traditionnellement l'apanage d'acteurs institutionnels dont l'objectif tient à l'étude des phénomènes de santé publique. Un droit « à la meilleure sécurité sanitaire au regard des connaissances médicales avérées » est mis en œuvre, selon les articles L. 1110-1 et L. 1110-5, alinéa 1 du Code de la santé publique. Les données qui sont recueillies en matière médicale participent à cette meilleure sécurité sanitaire et c'est notamment pour cette raison que la France, dès 1999, s'est dotée d'importantes bases de données en la matière, telles que le Système National d'Information Inter-régimes de l'Assurance Maladie (SNIIRAM) et le Programme de Médicalisation des Systèmes d'Information (PMSI). Définies respectivement aux articles L. 161-28-1 du Code de la sécurité sociale et L. 6113-8 du Code de la santé publique, ces bases de données nationales poursuivent différents objectifs, entre amélioration de la qualité de soins, contribution à une meilleure gestion de l'assurance maladie et des politiques de santé ou encore contrôle de la facturation.

Les données recueillies pour constituer ces bases sont des données individuelles nominatives qui sont en théorie anonymisées ou désidentifiées. Les noms et adresses ne figurent plus dans les bases de données et le numéro de sécurité sociale – le NIR – est remplacé par un identifiant propre pour éviter tout risque de ré-identification. Les textes en vigueur font ainsi référence à la notion de vie privée des individus ou aux modalités permettant de garantir leur anonymat. L'article L. 161-28-1 du Code de la sécurité sociale dispose que « les données reçues et traitées par le système national d'information interrégimes de l'assurance maladie préservent la vie privée des personnes ayant bénéficié des prestations de soins » et l'article L. 6113-8

[356] Isabelle De Silva, « Données, algorithmes et transparence des plateformes. Quels impacts sur la concurrence ? Quels enjeux pour la régulation ? (Retour sur les rendez-vous de l'Autorité de la concurrence du 24 nov. 2017) », *Dalloz IP/IT*, 2018, p. 8.

du Code de la santé publique concernant le PMSI insiste sur le besoin de respecter l'anonymat des patients.

174. Une surveillance par des opérateurs privés. La pratique de l'automesure contribue également à la création de bases de données mais celles-ci sont cette fois construites autour d'éléments récoltés directement par des opérateurs privés. Ces derniers mettent en œuvre des services et plateformes dédiées à la santé et servant à récolter les données agrégées par les objets connectés et applications utilisées dans le cadre de l'automesure. Le but de ces plateformes est simple puisqu'il s'agit de centraliser en un même lieu les données récoltées par les différents objets et applications.

Dans le cas d'*HealthKit*, plateforme développée par la firme américaine Apple, les données recueillies par le biais d'une application via l'Apple Watch ou l'IPhone sont centralisées et d'autres applications peuvent, en fonction des choix de l'utilisateur, y avoir accès. Reposant sur des interfaces de programmation applicatives (ou API pour *application programming interface*), celles-ci permettent « à un système source d'exposer ses données à des fins d'exploitation par d'autres systèmes »[357]. Ainsi, ces API peuvent permettre à des développeurs d'avoir accès à des données rendues disponibles par un fournisseur de services pour développer de nouveaux services ou de nouvelles fonctionnalités. Ce recours aux API ne permet pas, en théorie, l'accès aux données à caractère personnel détenues à l'origine par le responsable de traitement. Mais il est en revanche susceptible de fragiliser la sécurité informatique de la base de données en raison d'accès parfois non contrôlés de la part de tiers. A titre d'exemple, l'API du réseau social Facebook intégré au site de rencontre Tinder a permis, en 2018, l'accès aux informations de personnes inscrites sur le site[358]. Pour éviter de tels incidents, la concentration de données sensibles aux mains de nouveaux acteurs, rendue notamment possible par le recours généralisé à des algorithmes, doit entraîner la mise en place de mesures correctrices qui devraient permettre une meilleure classification des données collectées.

[357] Yves Tomic, « De l'usage des API. Les API de l'Abes », *Documentaliste-Sciences de l'Information*, vol. 51, no. 3, 2014, p. 17.
[358] Voir notamment : https://www.phonandroid.com/tinder-faille-de-securite-permet-pirater-n-importe-quel-compte-avec-numero-de-telephone.html

B. Des mesures correctrices à développer

175. La typologie des données à caractère personnel collectées, soumise au développement de solutions de *quantified-self*, est également précarisée en raison des liens qui sont tissés avec les autres dispositifs de santé connectée. L'automesure entretient en effet des rapports parfois ambigus avec cet écosystème, s'en rapprochant ou s'en éloignant, au gré des utilisations des dispositifs concernés. L'inclusion du *quantified-self* au domaine de la santé connectée est pourtant susceptible de fragiliser l'équilibre existant entre les différents types de régulation et doit conduire à l'adoption de mesures permettant d'expliciter les régimes juridiques applicables à chacune de ces activités. Dès lors, une clarification de l'écosystème de santé connectée semble nécessaire **(1)** et la prise en compte du contexte de création de la donnée doit être précisée pour assurer concrètement l'intelligibilité du cadre juridique applicable **(2)**.

1. Une clarification nécessaire de l'écosystème de santé connectée

176. La santé connectée ou e-santé, en plein développement, met en œuvre de nouveaux services qui reposent sur l'utilisation croissante d'outils numériques et de données. Également appréhendée sous le terme de cybersanté, celle-ci a été définie par l'OMS comme un procédé qui « consiste à utiliser, selon des modalités sûres et offrant un bon rapport coût/efficacité, les technologies de l'information et de la communication à l'appui de l'action de santé et dans des domaines connexes, dont les services de soins de santé, la surveillance sanitaire, la littérature sanitaire et l'éducation, le savoir et la recherche en matière de santé »[359]. Composante de la révolution numérique, le développement de l'e-santé est rendu possible grâce aux outils digitaux appliqués au domaine médicale ainsi qu'à la massivité et à la disponibilité des données. Ces éléments deviennent « le support de la médecine de demain […] que l'on peut dire « 5P » : préventive, prédictive, participative, personnalisée, pertinente »[360]. La e-santé entraîne un changement de paradigme dans la relation qui lie le patient au médecin. Ce dernier n'est plus à l'origine de

[359] Organisation Mondiale de la Santé, *Résolutions et décisions annexe*, Cinquante-Huitième Assemblée mondiale de la santé, Genève, 16-25 mai 2005, p. 114.

l'information qui va être délivrée en raison de la prise de conscience ou *empowerment* du patient.

177. Une redéfinition du rôle du patient. La mobilité croissante des individus a pu préfigurer le développement de ce type particulier de surveillance sanitaire[361]. La mission du médecin présente aujourd'hui plus un rôle de surveillance que de diagnostic et le patient devient lui « co-gestionnaire de la conception, de la mise en œuvre et du suivi d'un protocole de soins combinant un réseau d'acteurs, d'infrastructures et d'outils »[362]. Ce changement de paradigme quant au rôle du patient, conséquence du développement de l'e-santé, est en partie dû à la progression de la *m-health* ou santé mobile et qui représente donc à la fois une composante mais aussi une émanation de la santé connectée. A ce titre, la santé mobile recouvre « les pratiques médicales et de santé publique reposant sur des dispositifs mobiles tels que téléphones portables, systèmes de surveillance des patients, assistants numériques personnels et autres appareils sans fil »[363]. Cette définition de l'OMS rattache la santé mobile aux pratiques médicales ainsi qu'à la santé publique, mais elle présente pourtant un spectre plus large.

178. Un risque de segmentation de la protection. Cette définition permet en effet d'englober les applications concernant le mode de vie et le bien-être qui peuvent « se connecter à des dispositifs médicaux ou capteurs (bracelets ou montres), ainsi que les systèmes de conseil personnalisés, les informations de santé et rappels de prise de médicaments envoyés par SMS et la télémédecine pratiquée par communication sans fil »[364]. L'étude conduite par le cabinet d'avocats Hogan Lovells à la demande de la CNIL en 2013 relevait qu'il n'existait aucune loi spécifique à la santé mobile au niveau international. L'étude montrait cependant que plusieurs lois relatives à la e-santé et qui « qui traitent donc de tous les aspects numériques

---

[360] Julien Damon, « Révolution numérique : sécurité sociale 2.0 et médecine « 5P » », *RDSS*, 2017, p. 925.
[361] Jean-Philippe Lhernould, « Professionnels de santé et assurance maladie dans un espace européen sans frontières », *RDSS* 2010, p. 1004.
[362] Conseil National du Numérique, *La Santé, bien commun de la société numérique. Construire le réseau du soin et du prendre soin*, Rapport remis à la Ministre des Affaires sociales, de la Santé et des Droits des femmes, Octobre 2015, p. 7.
[363] Organisation mondiale de la santé, *mHealth, New horizons for health through mobile technologies*, Global Observatory for eHealth series, Volume 3, 2011, p. 6.
[364] Commission Européenne, *Livre vert sur la Santé mobile*, Bruxelles, avril 2014, p. 3.

touchant de près ou de loin à la santé, abordent les questions de régulation des applications de santé mobiles et de protection des données personnelles de m-santé »[365]. Un risque de segmentation de la protection est susceptible d'apparaître, entre recours à des lois sectorielles relatives à la réglementation de l'activité des professionnels de santé et lois générales portant sur la protection des données.

Cette segmentation de la protection, à laquelle l'automesure est soumise par sa position ambivalente et son rapprochement à d'autres éléments de santé connectée, peut entraîner un manque de visibilité des règles protectrices applicables. A l'origine destiné à mesurer des données relatives à l'activité sportive, le *quantified-self* peut pourtant s'inscrire dans un parcours de soins plus traditionnel. Les données qui en sont issues, considérées comme des données de santé, pourront ainsi faire l'objet d'un traitement par des professionnels de santé dans un cadre réglementé[366]. Mais ces données pourront aussi être considérées comme étant de simples données à caractère personnel et donc, faire l'objet d'une protection moindre. Une clarification des définitions et des règles applicables aux composantes de la santé connectée apparaît dès lors nécessaire pour garantir une certaine sécurité juridique aux individus et fournisseurs de services connectés. Celle-ci permettrait une meilleure prise en compte de la diversité des opérations réalisées dans le cadre de la santé connectée ou de la santé mobile et contribuerait ainsi à pouvoir déterminer avec plus de précision quel régime juridique est applicable. Le recours au contexte de création de la donnée peut dans certains cas aider à déterminer la nature des informations traitées, mais sa pertinence reste encore trop limitée.

2. La prise en compte limitée du contexte de création de la donnée

179. Outre la nature objective de la donnée de santé, il est dans certains cas fait référence au contexte de création de la donnée afin de déterminer la qualification juridique à retenir, à l'image du recours au principe de finalité déjà évoqué[367]. Certains responsables de traitement opérant dans le domaine du *quantified-self* précisent et intègrent cette distinction dans leurs conditions et politiques générales

[365] CNIL, *Le corps, nouvel objet connecté*, Cahiers Innovation & Prospective, 2014, p. 44.
[366] Cf., *supra*, n° 129.

d'utilisation. L'engagement de confidentialité de la société *Under Armour*, équipementier sportif, précisait avant l'entrée en application du RGPD qu'une « quantité très limitée des données de performance […] à savoir le nombre d'heures de sommeil de l'athlète et son rythme cardiaque, peut être considérée comme relevant des informations personnelles médicales en vertu de la Directive européenne de protection des données et de son interprétation par les autorités européennes de contrôle de la protection des données, si elles sont enregistrées pendant une durée prolongée »[368].

Cette précision permet d'abord de confirmer que des données en apparence non-sensibles peuvent le devenir lorsqu'elles sont collectées pendant une certaine durée. Mais ces éléments sont, pour le responsable de traitement, uniquement destinés à fournir des informations supplémentaires que l'individu peut intégrer à son évaluation vers ses « objectifs de forme et de bien-être ». Dès lors, même si des mesures du rythme cardiaque peuvent être réalisées par des appareils pouvant être reliés aux applications proposées, ces informations « ne doivent toutefois pas être considérées comme des conseils médicaux professionnels et ne doivent pas être utilisées à des fins de diagnostic »[369]. Dès lors, même si ces données doivent être considérées comme des données de santé, elles ne peuvent servir de fondement à un diagnostic médical.

180. Des régimes de protection différents pour une même donnée. Comme l'indique la CNIL, il serait pourtant « envisageable d'utiliser des données produites par les utilisateurs avec des outils de type *quantified-self* dans un contexte médical »[370]. A l'image des solutions déployées dans le cadre de la télémédecine, l'utilisateur d'un dispositif de *quantified-self* pourrait y recourir en vue de suivre son état de santé en dehors des murs de l'hôpital, mais sous la supervision d'un professionnel de santé. Cette distinction ne permettrait pourtant pas une protection

---

[367] Cf., *supra*, n° 144.
[368] Texte complet disponible en ligne à cette adresse : https://account.underarmour.com/privacy#le-type-d-informations-que-nous-collectons
[369] *Ibid.*
[370] CNIL, *op. cit.*, p. 15.

unifiée et objective des informations collectées. Elle serait en effet susceptible de soumettre des données similaires à des régimes protecteurs différenciés et un individu, pris en charge dans le cadre d'une structure de soins, serait dès lors davantage protégé qu'une personne s'automesurant dans un cadre privé ou dans un contexte ludique et sportif.

Le contexte médical est par nature plus protecteur que le cadre privé et le recours à la confidentialité instaurée dans le cadre du secret professionnel permet d'apporter certaines garanties supplémentaires aux individus, notamment pour les cas d'accès à des données personnelles de santé[371]. Ce cadre institutionnel protecteur, inexistant lorsque la collecte est réalisée dans un cadre privé, peut donc avoir pour effet de soumettre deux données identiques à des régimes de protection différents. Cette distinction est justifiée par des contextes de création et d'utilisation des données différents. Mais la collecte réalisée dans un cadre privé est fondée sur un service gratuit reposant sur une monétisation des données collectées. Les responsables de traitement utilisent en effet les données traitées à des fins publicitaires et commerciales. La collecte réalisée sera donc susceptible d'être hautement préjudiciable pour la personne concernée par de tels traitements.

SECTION II. L'INSUFFISANCE DU PRINCIPE DE FINALITÉ DANS LE TRACAGE DE CETTE FRONTIÈRE

181. La CNIL et l'AFCDP considèrent dans certaines hypothèses que la qualification d'une donnée de santé est susceptible d'être fonction de la finalité annoncée du traitement[372]. Cette solution trouve un écho particulier en matière de *quantified-self* au regard notamment de l'emploi d'objets connectés et d'applications collectant des données relatives soit au bien-être, soit à la santé et dont les critères de distinction sont parfois difficiles à mettre en œuvre. Le recours au principe de finalité doit dès lors permettre de distinguer entre d'une part, finalité sanitaire emportant la

[371] Cf., *infra*, n° 352.
[372] Cf., *infra*., n°387.

qualification de donnée de santé et d'autre part, finalité ludique emportant simplement la qualification de données à caractère personnel.

Ce recours au principe de finalité est également apprécié à l'aune de l'éventuelle qualification de dispositifs médicaux des objets connectés utilisés dans le cadre de l'automesure. A ce titre, la qualification de dispositif médical d'un smartphone a pu être envisagée par le passé, en raison notamment du capteur de rythme cardiaque intégré directement au sein de l'appareil[373]. Or, le recours au mécanisme légal protecteur associé aux dispositifs médicaux serait dans certains cas susceptible d'apporter une protection supplémentaire à l'individu souhaitant procéder à une automesure connectée. Pourtant, ce recours au principe de finalité est susceptible de présenter certaines limites, en particulier en raison du fait que c'est le responsable de traitement qui détermine lui-même cette finalité **(Paragraphe 1)**, mais également de son influence sur le principe de proportionnalité qui en découle directement **(Paragraphe 2)**.

§1. Une détermination subjective de la finalité du traitement et de l'objet utilisé

182. La finalité d'un traitement de données à caractère personnel est librement déterminée par le responsable de traitement qui choisit lui-même les raisons pour lesquelles il met en œuvre un tel traitement. Cette finalité doit simplement, au regard de l'article 5. 1 b) du Règlement général européen, être déterminée, explicite et légitime. Mais la notion de finalité est également utilisée pour déterminer la qualification de dispositif médical d'un objet connecté. Dans ce cas, le principe de finalité n'est plus appliqué au traitement ou à la donnée récoltée, mais directement à l'objet utilisé pour procéder à une telle collecte. Or, en matière de *quantified-self,* le fabricant de l'objet utilisé aura tout intérêt à écarter la finalité thérapeutique, médicale ou diagnostique de l'objet afin de commercialiser librement son dispositif **(A)**, montrant par la même occasion les limites du recours à un tel principe **(B)**.

[373] Guillaume Promé, « Galaxy s5 : La Corée envisage une certification médicale », *Qualitiso*, 13 mars 2014, accessible en ligne à cette adresse : http://www.qualitiso.com/galaxy-s5-dispositif-medical-coree/

A. L'exclusion du régime protecteur applicable aux dispositifs médicaux

183. La directive du 14 juin 1993 relative aux dispositifs médicaux définit le dispositif médical comme « tout instrument, appareil, équipement, matière ou autre article, utilisé seul ou en association, y compris le logiciel nécessaire pour le bon fonctionnement de celui-ci »[374]. Répertoriés en différentes classes selon leur niveau de dangerosité, les dispositifs médicaux font l'objet d'une réglementation au niveau national et européen, cette dernière ayant été actualisée par un Règlement en date du 5 avril 2017 qui complète et modifie la définition initiale donnée par la directive[375], reprise au sein de l'article L. 5211-1 du Code de la santé publique. Certains fabricants décident de recourir à la qualification de dispositif médical pour les objets qu'ils souhaitent commercialiser[376] mais ce choix leur est en théorie librement accordé. Dès lors, ceux-ci sont susceptibles de ne pas y procéder, en raison des lourdes contraintes pesant sur eux **(1)** ce qui peut entraîner une protection moindre pour les utilisateurs **(2)**.

1. Des contraintes renforcées pour le fournisseur du service

184. Chaque année, « environ 3000 dispositifs médicaux sont mis sur le marché français » ; ces dispositifs doivent recevoir un marquage dit « marquage CE », afin notamment « d'assurer la sécurité des consommateurs »[377]. Les dispositifs médicaux commercialisés font en effet l'objet d'une surveillance à trois niveaux. Celle-ci vise à mettre en place des processus permettant de détecter et de porter à la connaissance des autorités les évènements de sécurité sanitaire, à vérifier que ces processus ont été correctement définis et mis en place et enfin, à permettre à l'Agence nationale de Sécurité du Médicament et des produits de santé (ANSM) de réaliser des

[374] Article 1.2 a), Directive 93/42/CEE du Conseil, du 14 juin 1993, relative aux dispositifs médicaux.
[375] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE (Texte présentant de l'intérêt pour l'EEE).
[376] Voir par exemple le tensiomètre connecté de la firme *iHealth* qui est explicitement présenté comme un dispositif médical portant à ce titre un marquage CE.
[377] Centre d'analyse stratégique, *Le dispositif médical innovant*, La Documentation française, 2013, p. 51.

audits des organismes chargés de délivrer le marquage CE et de surveiller le marché ainsi que les évènements de sécurité sanitaire[378].

185. Une finalité déterminée par le fabriquant. La procédure de certification qui est mise en œuvre, longue et complexe, s'avère également coûteuse pour les fabricants de dispositifs médicaux. Ceux-ci doivent notamment « planifier, réaliser et documenter une évaluation clinique » afin de démontrer « la conformité aux exigences de sécurité et performance du règlement qui dépendent des caractéristiques et de la destination du dispositif »[379]. Le Règlement du 5 avril 2017 a apporté certaines précisions sur la notion de finalité médicale qui doit être associée au dispositif. Celle-ci doit être précise et découle de « la destination d'usage du dispositif telle qu'elle est voulue par le fabricant et indiquée sur l'étiquetage ou la notice d'utilisation »[380]. Par ailleurs, la nouvelle définition intègre les notions de prédiction et de pronostic au titre des usages potentiels des dispositifs médicaux, afin notamment de « répondre aux promesses de l'intelligence artificielle et du big data, avec le développement d'algorithmes prédictifs et pronostiques visant à accompagner la décision médicale »[381]. Les évolutions souhaitées en matière de médecine connectée semblent donc être prises en compte par la réglementation actualisée qui va dans le sens d'une reconnaissance du potentiel de la *e-health* dans le cadre de parcours de soins plus traditionnels.

186. Pour autant, ce renforcement du cadre juridique est susceptible de laisser certaines questions en suspens, notamment au regard de son applicabilité au cadre du *quantified-self* et aux objets et applications qui sont utilisés. En effet, étant dépourvus de finalité médicale, les applications et objets relevant du simple bien-être sont exclus de la qualification et de la règlementation de dispositif médical. Ainsi, « une application destinée à mesurer le rythme cardiaque ne sera pas considérée comme un dispositif médical si elle est destinée à être utilisée pendant la course à pieds alors qu'elle le sera si elle est destinée à la surveillance du rythme d'une personne atteinte

[378] *Ibid.*, p. 52.
[379] Haute Autorité de Santé, *Parcours du dispositif médical en France*, Guide pratique, novembre 2017, p. 12.
[380] Jérôme Peigné, « La notion de dispositif médical issue du règlement (UE) 2017/745 du 5 avril 2017 », *RDSS*, 2018, p. 5.
[381] *Ibid.*

d'insuffisance cardiaque »[382]. Le recours au principe de finalité est dès lors justifié pour procéder à une qualification subjective du dispositif utilisé, en fonction du choix du fabriquant et de son utilisation concrète et pratique. Pourtant, au regard non plus de l'objet utilisé mais des données qui sont traitées, celles-ci sont susceptibles de révéler *in fine* les mêmes informations. La règlementation relative aux dispositifs médicaux connectés ne préjuge pas de celle relative aux données à caractère personnel mais le suivi des dispositifs médicaux est susceptible de limiter le risque informationnel déjà envisagé.

187. Le décalage actuel entre les régimes juridiques applicables aux dispositifs médicaux et aux dispositifs de *quantified-self* est préjudiciable pour les individus. En effet, comme le relèvent certains auteurs, « le champ d'application de la réglementation apparaît aujourd'hui inadéquat, puisqu'une part non négligeable des logiciels de « santé connectée » va continuer à échapper au système[383]. Les applications utilisées dans le cadre de l'automesure sont dès lors susceptibles d'être écartées du dispositif protecteur puisque, selon le considérant 19 du Règlement renouvelant le cadre juridique applicable aux dispositifs médicaux, « les logiciels destinés à des usages généraux, même lorsqu'ils sont utilisés dans un environnement de soins, ou les logiciels destinés à des usages ayant trait au mode de vie ou au bien-être, ne constituent pas des dispositifs médicaux ». Dès lors, cette frontière nette entre dispositifs relatifs à la santé d'une part et dispositifs relatifs au bien-être d'autre part, « paraît en décalage avec les évolutions récentes, tant techniques que sociales »[384]. Ainsi, cette distinction entre bien-être et santé est, au regard des applications utilisées, susceptible d'entraîner des différences quant aux modalités de mise à disposition de telles applications.

188. Enfin, le recours à la qualification de dispositif médical ne semble pas avantageux pour les fabricants et développeurs d'application puisque « les perspectives de retour sur investissement sont suffisamment florissantes avec les applications récréatives et de bien-être » et que « le marché de la santé devient

[382] Deborah Eskenazy, *Le dispositif médical à la recherche d'un nouveau cadre juridique,* Thèse de doctorat de l'Université Lille 2 Droit et santé, Présentée et soutenue publiquement le 30 novembre 2016, p. 30.
[383] Paul-Anthelme Adèle, Sonia Desmoulin-Canselier, « Droit des dispositifs médicaux : vers une réforme ou un simple réaménagement ? », *RDSS*, 2016, p. 930.

exploitable dans des marges très rentables, sans avoir à s'astreindre aux exigences réglementaires »[385]. Ce mouvement semble dès lors s'opposer au fait que « de plus en plus de dispositifs médicaux impliquent des logiciels informatiques dont l'objet n'est pas d'agir directement sur le corps humain, mais de produire des informations physiologiques ou pathologiques le concernant »[386]. Cette inadéquation du cadre relatif aux dispositifs médicaux à celui de l'automesure connectée, également constatée pour les dispositifs médicaux de diagnostic *in vitro*[387], est donc susceptible de mettre en œuvre une protection moindre pour les individus concernés.

2. Une protection amoindrie de l'utilisateur

189. Des règles complémentaires. La règlementation relative aux dispositifs médicaux n'est pas exclusive de l'application de celle relative à la protection des données personnelles. Ces deux ensembles de règles sont au contraire complémentaires et le considérant 89 du Règlement du 5 avril 2017 indique que « le texte respecte les droits fondamentaux et les principes reconnus en particulier par la charte et, spécialement […] la protection des données à caractère personnel ». A ce titre, les article 109 et 110 du Règlement font directement référence aux règles issues de l'ancienne directive 95/46/CE en explicitant le fait que « toutes les parties concernées par l'application du présent règlement respectent la confidentialité des informations et données obtenues dans l'exécution de leurs tâches de manière à protéger les données à caractère personnel ». Le marquage CE qui est apposé sur les dispositifs pour « indiquer leur conformité avec le présent règlement afin qu'ils puissent circuler librement dans l'Union et être mis en service conformément à leur destination »[388] est susceptible de garantir une protection renforcée des données à caractère personnel en amont, au stade de l'évaluation des dispositifs médicaux.

---

[384] *Ibid.*
[385] *Ibid.*
[386] Jérôme Peigné, « Le nouveau cadre juridique des dispositifs médicaux », *RDSS*, 2018, p. 3.
[387] Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directives 98/79/CEE et la décision 2010/227/UE de la Commission, considérant 10.
[388] *Ibid.*, considérant 40.

190. La réalisation d'une investigation clinique. Certaines catégories de dispositifs médicaux nécessitent en effet, préalablement à leur commercialisation et à l'obtention du marquage CE, la réalisation d'une étude dite d'investigation clinique visant à étudier les impacts éventuels de la mise sur le marché de tels dispositifs. Dans ce cadre, les données issues de ces investigations cliniques font l'objet de mesures de protection complémentaire énoncées dans le Règlement du 5 avril 2017. Celui-ci précise dans son annexe XIV relative aux investigations cliniques que celles-ci doivent établir une « description des dispositions prises pour respecter les règles en matière de protection et de confidentialité des données à caractère personnel ». Parmi les informations devant être explicitées, on retrouve notamment les dispositions « organisationnelles et techniques qui seront mises en œuvre pour éviter l'accès non autorisé, la divulgation, la diffusion, l'altération ou la perte d'informations et de données à caractère personnel traitées »[389].

191. Une portée limitée. Le dispositif mis en œuvre dans le cadre de l'investigation clinique permet un renforcement *ex ante* des données à caractère personnel des individus. Mais sa portée, au regard de l'ensemble des catégories de dispositifs médicaux, semble pourtant limitée. En effet, son champ d'application, limité aux dispositifs médicaux de classe III, à savoir ceux qui présentent une certaine dangerosité, exclut par nature les dispositifs connectés de type objet connecté ou application, susceptibles d'être utilisés pour la pratique de l'automesure. Par ailleurs, le nombre important d'exceptions permettant de déroger à la nécessité de mettre en œuvre une investigation clinique en limite la portée. La notion d'équivalence permet, par exemple, de passer outre l'investigation clinique s'il existe déjà un dispositif médical équivalent sur le marché. Dès 2013, le Contrôleur européen de la protection des données souhaitait la précision et l'inclusion dans le texte du Règlement de certains éléments, relatifs notamment à la référence explicite aux données sensibles telles que décrites par l'article 8 de la directive de 1995 ou encore au rappel des droits des personnes concernées sur leurs données à caractère personnel[390].

[389] Annexe XIV, Règlement (UE) 2017/746.
[390] Contrôleur Européen de la Protection des Données, *Résumé de l'avis du Contrôleur européen de la protection des données sur les propositions de la Commission concernant un règlement relatif aux dispositifs médicaux, et modifiant la directive*

192. Une précision éventuelle sur la nature des données traitées. Le régime juridique applicable aux dispositifs médicaux semble en principe exclure les dispositifs de *quantified-self* de son champ protecteur. Mais il permet en revanche de préciser la nature des données en théorie collectées dans ce cadre. Le recours à la finalité sanitaire semble en effet mettre en œuvre une présomption de caractère sensible des données collectées. Le fait que ces dispositifs soient utilisés directement pour le bénéfice médical du patient, en fonction de l'intention du fabricant lors de la conception des applications proposés aux patients et professionnels de santé permettrait un traçage plus net de la frontière entre données personnelles classiques et données personnelles relatives à la santé. Ainsi, la finalité sanitaire expressément indiquée par le fabricant contribuerait à lever les doutes existant en cas de conflits potentiels de qualification au regard des données qui sont traitées[391].

La qualification éventuelle de donnée de santé pourrait donc, dans certains cas précis, être discutée en fonction de l'appareil qui produit cette donnée. En effet, « pour qu'une donnée puisse être utilisable dans un contexte médical, le dispositif qui produit cette donnée doit répondre à des normes strictes encadrées notamment par le Code de la santé publique ». Dès lors, « un dispositif répondant à ces normes sera réputé produire des données de santé même si celles-ci n'ont pas pour destinataire un professionnel de santé »[392]. Cette solution n'est pourtant pas retenue à l'heure actuelle et l'exclusion des dispositifs de *quantified-self* de ce cadre protecteur est révélatrice des limites du recours au principe de finalité pour la qualifications des données collectées.

B. L'insuffisance du rôle correcteur du principe de finalité

193. Le groupe de travail « Données de santé » de l'AFCDP, face aux difficultés soulevées par les conflits de qualification éventuelles portant sur les

---

2001/83/CE, le règlement (CE) no 178/2002 et le règlement (CE) no 1223/2009, et un règlement relatif aux dispositifs médicaux de diagnostic in vitro, Journal officiel de l'Union européenne, C 358/10, 7 décembre 2013.

[391] Jeanne Bossi Malafosse, « À partir de quand peut-on qualifier un logiciel de dispositif médical ? », *Dalloz IP/IT*, 2016, p. 82.

[392] AFCDP, *op. cit.*, p. 18.

données issues du *quantified-self*, considère que chaque situation nécessite d'être examinée au cas par cas. Cette appréciation porte sur le contexte de création et d'interprétation de la donnée mais également sur la finalité pour laquelle ces données sont collectées. Cette distinction permet d'identifier des données de santé lorsque celles-ci sont collectées pour des finalités sanitaires. Pourtant, le principe de finalité susmentionné se montre insuffisant pour parvenir à une qualification certaine des données, au regard notamment de sa libre détermination **(1)** et de la protection trop importante qu'il est susceptible de mettre en œuvre dans certains cas **(2)**.

1. Un principe à géométrie variable

194. Le recours au principe de finalité comme élément de détermination subjective de la nature des données à caractère personnel traitées serait susceptible de préciser certaines « zones grises » dont le développement est rendu possible par la pratique du *quantified-self*. L'inexistence juridique de la notion de bien-être ainsi que le traitement de données relatives à la santé sont susceptibles d'instaurer un doute quant à la qualification à retenir des données collectées. Or, le principe de finalité permettrait de tracer la frontière entre bien-être et santé, en fonction des modalités d'utilisation et de réutilisation de telles données. Recourir à cette méthodologie est pourtant porteur de risques. La détermination subjective de la qualification, qu'il s'agisse de l'objet utilisé ou des données collectées, soumet des informations révélatrices de l'état de santé à des régimes juridiques protecteurs distincts.

195. Des régimes juridiques opposés. Les traitements relatifs aux données personnelles traditionnelles d'une part et données à caractère sensible d'autre part, reposent sur des régimes juridiques diamétralement opposés. Dans un cas, c'est une liberté de procéder à un traitement qui est mise en œuvre, fondée sur l'effet libératoire du consentement donné par l'individu. Dans l'autre, il s'agit d'une interdiction de principe. Or, le recours au principe de finalité comme élément déterminant de la qualification est susceptible de remettre en cause cette distinction conceptuelle. L'exemple déjà avancé d'une application ou d'un dispositif connecté visant à mesurer des éléments relatifs à la course à pieds est particulièrement révélateur. Lorsque la finalité annoncée du traitement ou du dispositif utilisé est à

visée médicale, les données collectées auront vocation à recevoir la qualification de données de santé. Au contraire, la finalité ludique aura pour effet de retenir la qualification de donnée à caractère personnel simple.

196. Des informations similaires. Les données relevées sont pourtant susceptibles de révéler *in fine* le même type d'informations concernant l'individu. Dans le premier cas, la donnée relative à la foulée sera considérée comme une donnée de santé et son traitement, en principe interdit, reposera sur le consentement renforcé et explicite de l'individu. Dans un second cas, le traitement de cette même information, donnée identifiante classique, sera libre. Le responsable de traitement devra simplement s'acquitter de ses obligations légales. Les données collectées et traitées, bien que théoriquement identiques, seront pourtant soumises à des régimes juridiques protecteurs différents. Dès lors, la classification envisagée ne permet pas de préjuger du risque informationnel pesant sur les individus. Par ailleurs, la qualification dans ce cadre de simple donnée à caractère personnel n'empêche pas que celle-ci soit agrégée avec d'autres données et qu'elle puisse révéler *a posteriori* des éléments relatifs à la santé de l'individu. Ainsi, une donnée relative à la foulée, donnée à caractère personnel, pourra être corrélée avec des informations relatives au rythme cardiaque afin de révéler certains troubles de santé. Ce risque d'interconnexion de données, déjà envisagé[393], montre les insuffisances du recours au principe de finalité dans la qualification des données traitées.

2. Le risque d'une protection trop importante

197. Le principe de finalité, utilisé comme élément de qualification des données, semble parfois en décalage avec la réalité des distinctions à effectuer entre données à caractère personnel et données sensibles. C'est *in fine* l'hypothèse d'une qualification systématique des données collectées en données sensibles qui doit être envisagée. Celle-ci serait susceptible de limiter les innovations mises en œuvre dans

[393] Cf., *supra*., n° 158.

le cadre de l'automesure, selon la distinction déjà évoquée de principe de précaution et de principe d'innovation libre[394].

198. Un principe de précaution inadapté. Le principe de précaution, dont on trouve une illustration au sein de la Charte de l'environnement de 2004 intégrée à la Constitution aurait vocation à être mobilisée par la simple connexion des objets connectés utilisés pour la pratique de l'automesure[395]. Ainsi, le risque le plus évident serait de provoquer une « attitude frileuse chez les inventeurs » [396] empêchant un développement de l'innovation. En suivant les recommandations de l'article du groupe de l'article 29 qui propose de retenir la qualification de donnée de santé non seulement pour les données brutes permettant de tirer des conclusions sur l'état de santé d'une personne mais également pour les conclusions portées sur l'état de santé ou les risques éventuels relatifs à la santé[397], il serait dès lors possible de considérer que toutes les données produites dans le cadre de l'automesure connectée sont relatives à la santé et donc nécessitent une protection renforcée.

Les capacités de croisement et d'interconnexion des données dont les responsables de traitement bénéficient actuellement, associées aux capacités prédictives des algorithmes font que toutes les données identifiantes issues de l'automesure sont susceptibles de permettre la création d'informations relatives à l'état de santé d'une personne. Les données issues d'un pèse-personne connectée, associées à celle d'un podomètre, d'un compteur de calories ou d'une application relative à la qualité du sommeil de l'individu peuvent toutes avoir pour conséquence de dresser des conclusions relatives à la santé. Surtout, ces différentes mesures peuvent également être croisées à des données récoltées hors du cadre de l'automesure (applications de commande de repas à distance ou encore relatives à la pollution, par exemple) et qui permettront donc d'affiner les résultats issus de l'écosystème du *quantified-self*. Toute donnée issue de l'écosystème du *quantified-self* pourrait donc en théorie être soumise au régime juridique des données sensibles.

---

[394] Cf., *supra*, n° 142.
[395] Thierry Piette-Coudol, *op. cit.*, p. 25.
[396] *Ibid.*
[397] « If seemingly innocuous raw data are tracked over a period of time, combined with other data, or transferred to other parties who have access to additional complementary datasets, it may well be that even the seemingly most innocuous data, combined with other data sources, and used for other purposes, will come within the definition of 'health data' ».

Cette soumission systématique des données au régime des données sensibles pourrait ainsi limiter les bénéfices du *quantified-self* et empêcher un apport d'informations complémentaires à celles qui sont relevées dans le cadre strict du domaine médical.

199. Un lien avec la santé limité par l'absence d'exactitude des données collectées. L'article 5 d) du RGPD dispose que les données à caractère personnel doivent être « exactes et, si nécessaire, tenues à jour » en précisant que « toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ». Ce principe semble pourtant difficilement conciliable avec l'automatisation des traitements mis en œuvre dans le cadre de l'Internet des objets. Le G29 précisait que les conclusions relatives à l'état de santé devaient être considérées comme des données sensibles, sans égard pour leur fiabilité éventuelle. Mais la conciliation de cette interprétation avec le principe d'exactitude semble difficilement envisageable. Celui-ci est surtout révélateur des tensions qui existent entre le « tout santé » que la définition large des données de santé confère aux données issues de l'automesure et la réalité concrète.

L'équipementier sportif Under Armour, éditeur de différents services d'automesure (UA Record, MapMyFitness, MyFitnessPal…), indique explicitement collecter des « données de remise en forme et de bien-être » parmi lesquelles on peut retrouver celles relatives au poids, au niveau de forme physique, ou encore au rythme cardiaque[398]. Il est pourtant précisé, malgré la nature des données traitées et leur qualification certaine de donnée de santé, que les services « ne sont pas des dispositifs médicaux et les données qu'ils fournissent ne sont pas destinées à être utilisées pour des motifs médicaux ou pour diagnostiquer, traiter, soigner ou prévenir des maladies, affections ou blessures »[399].

200. Les données traitées dans le cadre de la pratique de l'automesure n'ont donc pas vocation à remplacer les informations obtenues en milieu hospitalier. Cette dissociation des domaines de l'automesure et de la santé semble, outre l'absence

[398] https://account.underarmour.com/fr-fr/privacy
[399] https://account.underarmour.com/fr-fr/terms-and-conditions#

d'expertise d'un médecin, en partie justifiée par l'absence de garanties quant à l'exactitude des données traitées. Celles-ci, représentation de l'activité, « peuvent ne pas être entièrement exacts, notamment en ce qui concerne les données sur les pas, le sommeil, la vitesse, la distance ou les calories »[400]. Ce sont pourtant ces informations, relevées en quantité importante, qui permettront de dresser des conclusions relatives à la santé de l'individu.

§2. L'inadéquation de la proportionnalité à la finalité

201. Le considérant 39 du Règlement général européen indique que « les données à caractère personnel devraient être adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées ». L'exigence de proportionnalité figure parmi les conditions de licéité d'un traitement de données à caractère personnel. Principe essentiel de la réglementation, celui-ci conditionne l'étendue des informations que les responsables de traitement peuvent collecter. Cette proportionnalité du traitement, appréciée à l'aune de la finalité annoncée du traitement **(A)**, joue également un rôle quant aux modalités de réutilisation des données à caractère personnel traitées **(B)**.

A. Une proportionnalité fonction de la finalité

202. La finalité d'un traitement de données à caractère personnel a des incidences sur la qualification éventuelle d'une donnée. Mais elle a également pour objet de définir l'ampleur de l'opération de collecte réalisée. Ainsi, le responsable de traitement ne peut collecter des données que si celles-ci sont utiles et nécessaires à la poursuite de la finalité annoncée en amont. L'utilisation d'objets connectés pour la pratique de l'automesure remet pourtant en question la pertinence de ce recours au principe de proportionnalité, contribuant par la même occasion à fragiliser la distinction entre données personnelles et données sensibles.

Le principe de proportionnalité semble en effet en contradiction avec le développement des *big data* qui consistent, par opposition à la proportionnalité, à

[400] *Ibid.*

recueillir un nombre de données toujours plus important pour des finalités encore non déterminées. Or, cette remise en cause du principe de proportionnalité, pourtant essentiel pour garantir aux individus que seules les données nécessaires au service utilisé seront collectées, favorise également l'établissement de conclusions relatives à l'état de santé. Plus le nombre de données d'automesure traitées sera élevé, plus il sera possible d'en déduire des éléments relatifs à la santé de l'individu. Dès lors, cette remise en cause du principe de proportionnalité dans le cadre du *quantified-self* **(1)** est susceptible de complexifier son application concrète **(2)**.

1. Une remise en cause de la proportionnalité du traitement

203. La proportionnalité du traitement réalisé par un responsable de traitement est appréciée à l'aune de trois critères mis en œuvre par la règlementation : adéquation, pertinence et limitation. Ceux-ci, fonction du principe de finalité, supposent que le responsable de traitement limite l'étendue des données collectées à celles qui sont nécessaire pour réaliser la finalité annoncée. Or, si le principe de finalité permet de juger du degré de proportionnalité des données collectées, le risque pour les individus est que la finalité annoncée soit la plus large possible afin que le responsable de traitement puisse collecter un nombre toujours important de données.

204. Le risque relatif à la proportionnalité a déjà été soulevée dans d'autres domaines[401], mais ce risque est également applicable au domaine des objets connectés utilisés pour la pratique du *quantified-self*. Appliqué à ce domaine, la question de la finalité annoncée en amont du traitement se révèle double. Celle-ci concerne d'une part, la formulation de la finalité du traitement et d'autre part, la proportionnalité des données traitées au regard de cette finalité. Un rôle de curseur est donc conféré à cette dernière, permettant de juger de la validité de l'étendue des données collectées.

205. Une finalité extensive. L'analyse des termes employés par les responsables de traitement dans la formulation de cette finalité au sein des différentes conditions générales d'utilisation montre bien qu'en matière de *quantified-self*, celle-ci est déterminée de façon large. L'application de course à pieds Runtastic,

appartenant à l'équipementier sportif Adidas, indique par exemple que les données personnelles collectées seront traitées afin de « fournir une expérience utilisateur harmonieuse ». De nombreux éléments sont couverts par cette formulation : authentification de l'utilisateur, suivi ou affichage des informations relatives à l'activité physique et sportive, performance des applications proposées ou encore recherche et développement[402]. Les responsables de traitement ont en effet tout intérêt à définir une finalité qui soit susceptible de couvrir un spectre large d'informations. Par ailleurs, déterminer avec précision une finalité permettant d'apprécier la proportionnalité du traitement semble paradoxal dans le domaine de l'automesure connectée. En effet, bien que certains responsables déterminent de façon précise les différentes finalités pour lesquelles des données sont traitées, la finalité associée aux données d'activité est souvent définie de manière large, empêchant qu'un véritable contrôle de proportionnalité puisse être mis en œuvre. A titre d'exemple, la politique de confidentialité du fabricant d'objets connectés My Kronoz indique :

> *« Nous conservons vos données d'activité pour les sauvegarder, et les utilisons pour vous fournir des prestations telles que des statistiques personnalisées de vos activités physiques, des programmes d'activités, etc. »*[403]

206. Des applications développées par des responsables de traitement situés outre-Atlantique et disponibles sur le marché européen ne précisent dans certains cas aucune finalité directe mais font simplement référence au bon fonctionnement du service mis en place qui lui-même mentionne la notion d'activité physique et de bien-être s'y rattachant. Par exemple, la politique de confidentialité de l'application Pacer indique simplement collecter des données pour mettre en œuvre et améliorer le service, celui-ci ayant pour but d'aider les utilisateurs à « vivre une vie plus saine et active »[404].

---

[401] Sylvie Peyrou-Pistouley, « La protection des données à caractère personnel dans l'ELSJ, work in progress... », *RTD eur*, 2010, p. 775.
[402] https://www.runtastic.com/fr/politique-de-confidentialite
[403] https://www.mykronoz.com/fr/fr/privacy-policy/
[404] https://www.mypacer.com/privacy/ios/

207. Une finalité fondée sur la notion de bien-être. Certains engagements de confidentialité et conditions générales d'utilisation se montrent plus précis au regard de la finalité avancée en faisant directement référence au bien-être de l'individu. Par exemple, l'équipementier sportif Under Armour précise, dans sa politique de confidentialité :

> *« Under Armour recueille, utilise, divulgue et traite les données personnelles comme décrit dans la présente politique de confidentialité […] pour vous offrir des services de remise en forme et de bien-être innovants »*[405].

La référence à la notion de bien-être en tant que finalité est susceptible d'engendrer des difficultés d'appréciation au regard de la proportionnalité des données collectées. En effet, la notion de bien-être ne faisant l'objet d'aucune définition juridique dans le cadre de la protection des données à caractère personnel, celle-ci ne permet pas de préjuger de la nature des informations collectées. L'étendue potentielle du domaine du bien-être rend dès lors difficile l'appréciation de la pertinence des données collectées dans ce cadre. Certains objets connectés ou applications sont développés pour répondre à des besoins spécifiques, précisés par la finalité annoncée du traitement : calcul de la distance parcourue lors d'une course à pieds associé au nombre de calories dépensées ou nombre de calories ingérées lors d'un repas. Mais le recours au champ lexical du bien-être laisse la voie libre à une collecte élargie de données, en l'absence de définition juridique précise de la notion.

208. Une notion librement déterminée. Laisser la notion de bien-être à la libre appréciation d'entreprises du numérique développant des applications de mesure du bien-être ou des *trackers* d'activité et agissant en tant que responsables de traitement permet d'accroître le risque informationnel pesant sur les individus. Ces derniers sont en effet susceptibles de dévoiler un nombre important d'informations personnelles, nombre de pas parcourus en une journée, régime alimentaire ou encore activité relative au sommeil ou à la vie sexuelle. Bien que pertinent au regard de la quantification du bien-être, d'autres éléments, dont le lien est moins évident (tel le

[405] https://account.underarmour.com/fr-fr/privacy

cas de la géolocalisation enclenchée pour une application relative au sommeil), procèdent à une remise en cause de la pertinence des données collectées.

2. Une qualification fonction de la proportionnalité

209. La proportionnalité du traitement mis en œuvre est susceptible d'avoir des conséquences sur la qualification juridique des données collectées. En effet, plus la finalité annoncée du traitement de données sera formulée de manière large, plus le nombre d'informations permettant d'atteindre cette finalité sera important. Dès lors, le responsable de traitement aura accès à un nombre élevé d'informations et sera donc en mesure de déterminer des profils plus détaillés des individus utilisant ses services. Ce faisant, il pourra tirer plus facilement des conclusions relatives à l'état de santé des individus. En effet, la qualification appliquée aux données à caractère personnel sera susceptible de varier en fonction de la proportionnalité des données traitées.

210. Le G29 a considéré que sont identifiées au titre des données de santé les conclusions relatives à l'état de santé d'une personne qui sont réalisées à partir de données brutes. Or, le flux important d'informations collectées en vertu d'une finalité large et donc proportionnel à cette finalité permettra de déterminer plus facilement ces conclusions relatives à l'état de santé d'un individu. L'inexistence de critères précis permettant d'apprécier la portée juridique de la notion de bien-être est à nouveau susceptible de précariser la distinction entre les deux catégories juridiques de données. En effet, déterminer la proportionnalité des données collectées en fonction de la mesure du bien-être rend plus souple l'appréciation des critères relatifs à l'adéquation, à la pertinence ou au caractère non-excessif des données traitées. Par ailleurs, l'objectif du *quantified-self*, reposant sur une évaluation constante d'informations relatives au corps humain en vue d'en tirer des conclusions sur le bien-être de l'individu, semble théoriquement opposé à l'idée d'une proportionnalité des données traitées.

211. Une modification *a posteriori* de la nature des données. La classification des données proposée par le G29, reprise dans une moindre mesure par

le RGPD bien que confirmée par la CNIL[406], rend l'identification *ex ante* des données collectées complexe, en raison de la difficulté à déterminer avec précision et en amont leur nature. Ces données, collectées au moment de leur traitement initial, relève du régime juridique de droit commun des données à caractère personnel. Mais le spectre étendu de la finalité déterminée et donc l'éventuelle appréciation élargie de la proportionnalité du traitement et des éléments le composant sont susceptibles de modifier *a posteriori* la nature des données collectées. Cette modification *a posteriori* de la nature des données est source d'insécurité juridique pour les individus. Ceux-ci peuvent raisonnablement s'attendre à ce que des données simplement identifiantes soient traitées. Mais ils ne sont pas en mesure de prévoir que l'étendue des données collectées contribuera à révéler des éléments relatifs à leur état de santé, bien que certains responsables de traitement prévoient directement cette possibilité au sein de leurs conditions générales d'utilisation[407].

Les applications et les objets connectés, dont les conditions générales d'utilisation précisent qu'un changement potentiel de qualification des données est possible, sont peu nombreuses. Dès lors, se pose la question de la pertinence des principes de finalité et de proportionnalité au regard des autres conditions de mise en œuvre de collecte et de traitement.

B. Des modalités de collecte soumises au principe de finalité

212. Le principe de finalité, confronté au *big data*, est révélateur de la précarisation du cadre juridique applicable aux données à caractère personnel. Mais d'autres principes protecteurs sont également influencés et précarisés par le développement des objets connectés utilisés dans le cadre du *quantified-self*. En effet, le principe de finalité, utilisé pour déterminer la nature des données collectées, a également vocation à influencer les autres principes cardinaux de la règlementation mise en œuvre. Cette influence, qui peut être directe ou indirecte, se manifeste d'une

[406] https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante
[407] L'équipementier sportif *Under Armour*, développeur de l'application *My Fitness Pal,* indique à ce titre que certaines données de remise en forme et de bien-être recueillies, « à savoir, le nombre d'heures de sommeil de l'athlète et son rythme cardiaque, peuvent être considérées comme relevant des informations personnelles médicales en vertu du RGPD et de son interprétation par les autorités européennes de contrôle de la protection des données, si elles sont enregistrées pendant une durée prolongée ».

part à l'égard de la portée du consentement donné par la personne concernée par le traitement **(1)** et d'autre part, à l'égard de la détermination de la durée de conservation des données collectées **(2)**.

1. Une influence sur le consentement donné par l'individu

213. La nécessité d'un consentement renforcé. L'intérêt de la distinction entre les catégories juridiques relatives aux données personnelles traditionnelles et aux données personnelles sensibles repose sur l'appréciation du consentement donné par l'individu concerné. Dans un premier cas, une liberté de principe du traitement est envisagée, à condition d'obtenir le consentement de l'individu[408]. Dans un second cas, le traitement des données sensibles fait l'objet d'une interdiction de principe, levée par le recours au « consentement explicite » de la personne concernée par le traitement, en vertu notamment de l'article 9 du RGPD. Le consentement explicite, auquel l'article 6 de la LIL fait référence par renvoi au RGPD, s'entend d'un consentement à l'intensité renforcée et censé témoigner de la connaissance, par l'individu, que des données à caractères sensibles, relatives à l'intimité et présentant des risques particuliers sont traitées. La nature du consentement donné doit donc apporter une protection renforcée aux individus lorsque des données sensibles sont collectées.

214. Un consentement fonction de l'information délivrée. Le consentement est fonction de l'information qui est délivrée en amont à l'individu. Or, avec les objets connectés et applications de *quantified-self*, les modalités de délivrance de l'information sont susceptibles d'influencer et de fausser les conditions relatives au recueil du consentement et permettant la mise en œuvre du traitement. En effet, l'information délivrée à l'individu, préalablement ou concomitamment au recueil du consentement, ne porte pas directement sur la nature des informations traitées. Cette information concerne plus généralement l'opération de traitement mise en œuvre et notamment la finalité pour laquelle les données sont traitées ou collectées. Pourtant, les recommandations du groupe de l'article 29 relatives au consentement ont estimé que, pour être valablement obtenu, celui-ci doit être fondé sur une information

incluant le type de données collectées et traitées[409]. Selon cette interprétation, la personne concernée par le traitement de données à caractère personnel devrait savoir, à l'avance, quelle catégorie de données seront collectées. Le caractère sensible des données collectées devrait ainsi être clairement mentionné afin que les conditions relatives au recueil d'un « consentement explicite » soient remplies. Un encart au sein des engagements de confidentialité pourrait par exemple préciser qu'une application collecte des données relatives au rythme cardiaque, données considérées comme sensible par la réglementation.

215. Un consentement fragilisé. Requis lorsqu'un risque sérieux relatif à la protection des données est susceptible d'apparaître, le consentement explicite, selon l'interprétation donnée par le G29, se réfère à la façon dont le consentement est exprimé par la personne concernée par le traitement. La délivrance d'un écrit attestant du consentement au traitement est une solution efficace mais celle-ci n'est pas la seule, à l'image par exemple de l'envoi d'un courrier électronique, d'une signature électronique ou encore d'un formulaire en ligne à compléter. Le recours au consentement explicite est cependant fragilisé par les finalités larges mises en œuvre dans le cadre de l'automesure ainsi que par les modalités d'appréciation de la proportionnalité desdits traitements au regard de la finalité.

Le consentement explicite requis lorsque des données sensibles sont collectées doit être exprimé antérieurement à la mise en œuvre du traitement. Pourtant, l'hypothèse selon laquelle des données brutes non-sensibles sont susceptibles de révéler, par leur nombre important, des informations relatives à l'état de santé, vient remettre en question la distinction fondée sur le caractère progressif du consentement. Un responsable de traitement procédant à une collecte de données dénuées de caractère sensible pourrait échapper à l'exigence relative à l'obtention d'un consentement explicite : les données, dépourvues de caractère sensible au jour du traitement initial, ne nécessiteront qu'un consentement simple de l'individu, selon les modalités renouvelées par le RGPD. Cependant, l'évolution du traitement peut

[408] Cf., *infra*, n° 309.

changer la donne et contribuer à la création de données sensibles. Dès lors, même si le traitement initial n'a pas pour finalité immédiate de révéler des éléments relatifs à la santé de l'individu, le traitement ultérieur permettant d'y procéder devra répondre aux dispositions de l'article 13.3 du texte européen[410]. Le responsable de traitement devra dès lors préciser, au jour de la collecte initiale, que les informations collectées peuvent avoir pour finalité de révéler des informations relatives à la santé. Un consentement explicite sera donc exigé et l'information délivrée à la personne concernée devra mentionner cette finalité relative aux conclusions sur l'état de santé. Cette information relative à la révélation de données de santé est rarement mentionnée par les conditions générales d'utilisation et engagement de confidentialité des différentes applications d'automesure. Généraliser cette précision au sein des différents engagements de confidentialité constituerait une amorce de solution.

Les modalités de recueil du consentement explicite sont dans certains cas conformes aux dispositions renouvelées du cadre européen. Pourtant, une certaine clarification de ces modalités s'impose, dans le but notamment d'assurer une meilleure sécurité juridique aux individus ainsi qu'une meilleure prévisibilité des usages susceptibles d'être réalisés de leurs données à caractère personnel. Outre ces problématiques relatives aux différentes intensités du consentement requis, l'appréciation du principe de finalité a également des conséquences sur la durée de conservation des données à caractère personnel.

2. La détermination de la durée de conservation des données

216. Une durée de conservation théoriquement limitée. La loi Informatique et Libertés ainsi que le RGPD mettent en œuvre une obligation de limiter au strict minimum la durée de conservation des données. La loi Informatique et Libertés ainsi que le RGPD mettent en œuvre une obligation de limiter au strict minimum la durée de conservation des données. Ce principe de durée limitée de conservation était déjà

[409] Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679, WP 529, Adopted on 28 November 2017 P. 13.

avancé par l'article 5, e) de la Convention du Conseil de l'Europe du 28 janvier 1981 selon lequel « les données à caractère personnel faisant l'objet d'un traitement automatisé sont […] conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées ». Cette limitation temporelle du traitement apparaît comme le corollaire du principe de proportionnalité des données, cette obligation étant appréciée au regard de la finalité déterminée du traitement[411].

Les données à caractère personnel qui sont collectées doivent en théorie être conservées tant que la finalité annoncée du traitement n'est pas atteinte ou réalisée. Ainsi, comme l'a indiqué la CNIL dans une notice relative à la limitation de la conservation des données, « une fois que l'objectif poursuivi par la collecte des données est atteint, il n'y a plus lieu de conserver les données et elles doivent être supprimées »[412]. Fondement juridique permettant la mise en œuvre effective d'un droit à l'oubli ou droit à un déréférencement, cette durée limitée de conservation des données est justifiée par la nécessité de garantir aux individus une certaine maîtrise informationnelle[413]. Pourtant, cette durée de conservation des données, dépendante de la formulation du principe de finalité déterminée et de la proportionnalité du traitement mis en œuvre, est aujourd'hui remise en cause par le développement du *quantified-self* en raison des finalités avancées et de l'automatisation du processus de collecte.

217. Une durée appréciée largement en pratique. Le but de l'automesure connectée est de pouvoir procéder à une collecte permanente et continue de données à caractère personnel. Or, la précision des informations collectées est améliorée par leur accumulation dans le temps. En effet, plus la collecte de données est étendue chronologiquement, plus l'utilisateur d'un service de *quantified-self* sera en mesure d'apprécier les avancées de son effort physique, de son rythme de sommeil, de son

---

[410] Cet article précise que « lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité ».
[411] CNIL, *Guide employeurs*, p. 4.
[412] CNIL, *Limiter la conservation des données*, accessible en ligne à cette adresse : https://www.cnil.fr/fr/limiter-la-conservation-des-donnees.
[413] Cf., *supra*., n° 27.

poids ou encore de ses habitudes alimentaires. Le nombre d'informations à disposition devient donc le corollaire de l'efficacité du service puisqu'il permet une meilleure visibilité des progrès réalisés.

L'accumulation dans le temps de ces informations devient un gage d'efficacité du service puisqu'il permet à la personne concernée de réaliser un certain nombre de comparaisons. En effet, pour permettre par exemple à un coureur de mesurer l'évolution de ses progrès, celui-ci devrait pouvoir avoir accès à l'ensemble des mesures concernant ses différentes courses[414]. Il devient alors nécessaire de conserver l'ensemble des mesures réalisées pour proposer à l'individu un service qui soit le plus efficace possible et permette de mesurer valablement l'évolution des progrès réalisés. Un exemple similaire peut-être donné concernant un pèse-personne connecté. Son utilité réelle sera de pouvoir évaluer dans le temps l'évolution du poids, en comparant perte ou gain par rapport à une mesure initiale. Appréciée par rapport à la finalité annoncée du traitement, cette durée de conservation limitée est théoriquement susceptible de varier en fonction des objectifs annoncés du traitement et déterminés en amont par le responsable dudit traitement.

218. Le développement du *quantified-self* et sa connexion grâce aux dispositifs de l'Internet des objets rend ainsi complexe la détermination d'une durée de conservation des données, entendue comme « le temps qui sépare le moment de la collecte (ou de la génération d'une donnée) de son effacement complet du traitement »[415]. Le fait que des données à caractère personnel soient conservées par le responsable du traitement est en principe justifié par la possibilité qui doit lui être laissé de réaliser la finalité du traitement. Or, plus cette finalité sera exprimée de façon vague ou large, plus la durée de conservation pourra être également appréciée de façon large. Dès lors, il devient difficile d'apprécier la légalité de la durée de conservation des données à caractère personnel lorsque la finalité annoncée est relative au bien-être de l'individu. Appréciée subjectivement, cette finalité relative au bien-être pose la question de savoir à quel instant elle peut être considérée comme atteinte, en l'absence de tout élément concret d'appréciation.

[414] Voir annexe n°1.
[415] AFCDP, *Document de base sur la conservation des données*, 2011, p. 1.

219. Une exception fondée sur l'archivage. Un certain nombre d'indications, notamment en matière de données sensibles traitées dans un cadre médical[416], permettent d'apprécier la légitimité d'une durée de conservation des données à caractère personnel. Mais la conservation des données n'est autorisée que dans des cas très limités par la loi. Surtout, le responsable de traitement qui ne respecterait pas le délai déterminé en amont est susceptible de faire l'objet de sanctions pénales, l'article 226-20 du Code pénal disposant que « le fait de conserver des données à caractère personnel au-delà de la durée prévue […], est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques ».

Entendu par le Règlement général comme « toute opération de collecte et de traitement de données à caractère personnel nécessaires pour des enquêtes statistiques ou la production de résultats statistiques », ces fins statistiques impliquent cependant que « le résultat du traitement à des fins statistiques ne constitue pas des données à caractère personnel mais des données agrégées »[417]. En vertu de l'article 89 du même texte, ce traitement doit faire l'objet de garanties visant à « la mise en place de mesures techniques et organisationnelles, en particulier pour assurer le respect du principe de minimisation des données ». La CNIL, en 2005, a eu l'occasion de préciser quelles sont les règles applicables à l'archivage par des acteurs privés en distinguant archives courantes, intermédiaires et définitives[418]. Seules les archives courantes et intermédiaires – relatives à des données d'utilisation courante ou présentant encore un intérêt pour les services – sont soumises à des durées de conservation limitées, contrairement aux archives définitives qui présentent un intérêt historique, scientifique ou statistique, justifiant qu'elles ne fassent l'objet d'aucune destruction.

220. Conclusion du chapitre. L'automesure connectée met en œuvre un certain nombre de services innovants reposant sur une tentative de quantification

[416] CIL, *Référentiel durée de conservation*, juillet 2014, p. 7.
[417] Considérant 162, Règlement (UE) 2016/679,
[418] Délibération n° 2005-213 de la CNIL du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel.

objective du bien-être de l'individu. Pour y parvenir, différents services sont proposés et ils permettent une collecte d'informations, identifiées par la règlementation comme étant des données à caractère personnel. Pourtant, la notion de bien-être, absente de la législation relative à la protection des données, sème le doute quant à la véritable nature juridique des informations collectées, entre données à caractère personnel et données sensibles relatives dans certains cas à la santé. Les données collectées, rendues difficilement identifiables par le nombre et l'interconnexion de dispositifs utilisés, sont également soumises à un problème de classification, entretenu par la référence à la notion de bien-être dans les engagements de confidentialité. Or, la pratique de l'automesure, outre une identification plus complexe des données traitées, fragilise également le cadre juridique qui leur est applicable.

221. Conclusion du titre. L'automesure connectée est une pratique que le droit peine aujourd'hui à identifier pleinement. Les différents outils utilisés, en procédant à une collecte inégalée d'informations, ont influencé les définitions employés par le cadre juridique. Celles-ci ont évolué pour que le dispositif protecteur puisse s'appliquer largement et s'adapter, en théorie, aux nouvelles pratiques et aux nouveaux moyens de collecte de données. Le RGPD, en précisant dans un texte juridique contraignant la définition de donnée de santé, aurait dû permettre d'évacuer certains doutes subsistants. Mais le spectre élargi des définitions proposées laisse encore aujourd'hui certaines questions en suspens. En effet, les capacités d'analyse dont disposent à l'heure actuelle les dispositifs connectés font que toutes les informations sont susceptibles de devenir des données à caractère personnel, elles-mêmes susceptibles de devenir, par interconnexion ou corrélation, des données sensibles relatives à la santé. Le lien avec le bien-être, privilégié par le *quantified-self*, entretient ce doute et contribue à limiter l'efficacité des mesures protectrices instaurées.

TITRE II – LA PROTECTION LIMITEÉ DES DONNÉES D'AUTOMESURE CONNECTÉE

222. Les mécanismes de fonctionnement des objets connectés utilisés pour la pratique de l'automesure sont particulièrement révélateurs des tensions auxquelles le cadre juridique relatif à la protection des données est soumis.

Ils concentrent et cristallisent en effet un certain nombre d'évolutions technologiques : automatisation des processus de collecte, permanence des traitements réalisés, interconnexion des données collectées ou encore capacités d'analyse des informations et dialogue entre différents supports numériques. Cette technicité et cette complexité croissante des différentes opérations de traitement et de collecte vont de pair avec l'idée, pour les individus, d'une « transparence par les données comme voie de l'exploration de soi »[419]. Fondée sur une logique de « management de soi » ou *self-help*, la réalisation de cet objectif d'une meilleure connaissance de l'individu s'accompagne du recours à un nombre croissant d'acteurs collectant des données.

223. La recherche d'évaluation du comportement fait en effet intervenir des tiers disposant d'importantes ressources économiques et matérielles. La mise en chiffre de soi, rendue possible par une révélation toujours plus importante de données touchant à l'intimité, s'appuie sur des services proposés par des opérateurs privés. L'automesure connectée se « placerait donc dans la continuité de la surveillance par un gardien imaginé dans un dispositif panoptique »[420], les plateformes du numérique jouant le rôle du gardien tel qu'il est figuré dans les travaux de Jérémy Bentham[421].

Les fournisseurs de services opérant dans le cadre de l'automesure connectée entendent en effet, à l'image de certains réseaux sociaux ou moteurs de recherche,

[419] Eric Dagiral, Christian Licoppe, Olivier Martin *et al.*, « Le *Quantified Self* en question(s). Un état des lieux des travaux de sciences sociales consacrés à l'automesure des individus », *Réseaux*, 2019/4, n° 216, p. 17-54.
[420] *Ibid.*
[421] Jérémy Bentham, *Panoptique*, Fayard, 2002, 72 p.

s'établir en tant que véritables plateformes dont le but est de maximiser le nombre de données collectées, à travers des services aux capacités d'interopérabilités élevées[422].

Outre des risques relatifs à la sécurité des données[423], la collecte exponentielle d'informations conduit au développement d'un risque informationnel **(chapitre 1)**, révélateur de l'insuffisance des principes de protection **(chapitre 2)**.

[422] Boris Paulin, « La restitution des données : difficultés pratiques », *Dalloz IP/IT*, 2017, p. 33.

CHAPITRE I – LE DÉVELOPPEMENT D'UN RISQUE INFORMATIONNEL

224. L'ensemble des règles relatives à la protection des données à caractère personnel n'a pas pour but premier d'interdire tout traitement éventuel de données. Un encadrement de ces traitements est en revanche prévu afin de garantir certains droits aux individus. Le juste équilibre entre liberté de traitement et respect de droits et obligations doit conduire les individus à pouvoir maîtriser l'utilisation qui sera faite de leurs données. Le risque informationnel qui pèse sur les individus, entendu comme une perte de maîtrise des informations les concernant, est pourtant rendu difficilement maîtrisable par la quantité d'informations traitées à l'ère des *big data*. Le moindre coût des dispositifs utilisés contribue à démocratiser la pratique de l'automesure et favorise ainsi la création généralisée d'informations facilement exploitables. Aussi diverses que détaillées, ces informations permettent d'établir, en raison des modalités de profilage et du recours aux algorithmes, des profils très précis des individus auxquels elles se rapportent.

225. Le principe d'autodétermination informationnelle. Les données deviennent le moteur principal des services développés dans le cadre de l'économie numérique, selon l'idée parfois avancée d'un capitalisme de la surveillance[424]. Levier économique, les données collectées par les développeurs de service d'automesure peuvent être utilisées afin de modifier les comportements des individus. Celles-ci permettent également de proposer une publicité toujours plus ciblée et le modèle économique mis en œuvre, reposant sur la fourniture de données par l'individu en l'échange de services apparemment gratuits, contribue au renforcement de ce paradigme. L'activité d'individus pratiquant l'automesure est créatrice d'une valeur économique directement exploitable par des opérateurs privés. L'enjeu du droit à la

[423] Conseil d'Etat, *Puissance publiques et plateformes numériques : accompagner l'ubérisation*, Etude annuelle 2017, La Documentation française, p. 65.

protection des données est alors de permettre aux individus de maîtriser les informations qu'ils divulguent, parfois inconsciemment[425], selon le principe d'autodétermination informationnelle. D'abord apparu en Allemagne de façon prétorienne, ce principe traduit « la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel »[426]. Repris par le Conseil d'Etat dans un rapport de 2014, l'autodétermination informationnelle est envisagée comme la possibilité, pour l'individu, de contrôler l'étendue des données qu'il divulgue ainsi que les modalités selon lesquelles celles-ci sont réutilisées.

226. Le droit à l'autodétermination informationnelle. L'article 1er, alinéa 2, de la loi Informatique et Libertés dispose :

> *« Les droits des personnes de décider et de contrôler les usages qui sont faits des données à caractère personnel les concernant et les obligations incombant aux personnes qui traitent ces données s'exercent dans le cadre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 et de la présente loi ».*

L'autodétermination informationnelle semble donc avoir été consacrée en tant que droit-créance, entendu comme « la prétention légitime à obtenir les interventions requises pour que soit possible la liberté »[427]. Dette positive, ce droit à l'autodétermination informationnelle implique une intervention. Il constitue un objectif à atteindre[428] et « donne sens à tous ces droits, qui tendent à le garantir et doivent être interprétés et mis en œuvre à la lumière de cette finalité » [429]. Le droit à

---

[424] Shoshana Zuboff, *The age of surveillance capitalism : the fight for a human future at the new frontier of power*, Public Affairs, janvier 2019, 704 p.
[425] Cf., *supra*, n° 101.
[426] BVerfGE 65, 1 – Volkszählung Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. Und 19. Oktober 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden.
[427] Georges Burdeau, *Les libertés publiques*, LGDJ, 1961, p. 21.
[428] Laurence Gay, « La notion de « droits-créances » à l'épreuve du contrôle de constitutionnalité », *Cahiers du Conseil constitutionnel*, n° 16, juin 2004, p. 148.
[429] Conseil d'Etat, *Le Numérique et les droits fondamentaux*, Rapport Annuel, 2014, p. 267.

l'autodétermination permet de poser les bases de « l'ensemble de l'édifice juridique de la protection des données, impliquant par la suite de développer à la fois des outils adaptés à l'exercice de ses droits par la personne et à une nouvelle régulation »[430].

227. Pourtant, la croissance exponentielle d'informations collectées par la pratique de l'automesure semble rendre illusoire toute tentative de maîtrise des informations divulguées. Le modèle *freemium* mis en œuvre, lorsque le paiement d'un prix pour accéder à un service n'est requis que pour l'obtention de fonctionnalités complémentaires, contribue à cette divulgation et à l'opacité qui entoure parfois les opérations de collecte. Cette absence concrète d'autodétermination informationnelle **(section 1)** est ainsi renforcée, à l'heure actuelle, par l'existence d'une asymétrie informationnelle entre responsables de traitement et individus **(section 2)**.

[430] Edouard Geffray, « La protection des données personnelles, élément clé à l'ère du numérique », *Légipresse*, oct. 2014, n° 320.

SECTION I. L'ABSENCE D'AUTODÉTERMINATION INFORMATIONNELLE

228. L'article 54 de la loi pour une République numérique adoptée le 7 octobre 2016 est venue modifier l'article premier de la loi Informatique et Liberté pour y introduire la notion de contrôle des usages qui sont faits des données à caractère personnel. Cette nouvelle disposition est une formulation concrète du droit à l'autodétermination informationnelle. Elle montre qu'il « s'agit de passer d'une posture uniquement défensive de protection des données personnelles à une posture plus offensive de maîtrise, de contrôle et plus encore de capacité pour l'utilisateur à mobiliser et utiliser ses données pour ses propres finalités »[431].

Cette faculté de maîtrise pour les individus de leur vie en ligne est pourtant confrontée aujourd'hui aux transformations des usages numériques des données personnelles. En effet, les nanotechnologies rendent les systèmes invisibles, innombrables et « l'économie moderne repose dorénavant sur l'exploitation à grande échelle des données personnelles »[432]. Or, à travers la question de la valorisation des données apparaît également celle relative à leur appropriation. Le droit à l'autodétermination informationnelle s'oppose en théorie à la reconnaissance d'un droit subjectif de l'individu sur ses données **(Paragraphe 1)** et la reconnaissance de droit de la personnalité est, en Europe, privilégiée **(Paragraphe 2)**.

§1. Le rejet de la thèse de la propriété

229. Le droit à l'autodétermination informationnelle « offre certains avantages comparativement à la simple reconnaissance d'un droit subjectif de l'individu sur ses données », car il permet notamment « d'affirmer la primauté de la personne qui doit être en mesure d'exercer sa liberté »[433]. Pourtant, il a été suggéré qu'un droit de

[431] Assemblée Nationale, *Projet de loi pour une République numérique, Etude d'impact*, 9 décembre 2015, p. 97.
[432] Henri Oberdorff, « L'espace numérique et la protection des données personnelles au regard des droits fondamentaux », *Revue du Droit public, n°1*, 2016, p. 41.
[433] Nathalie Martial-Braz, « Le renforcement des droits de la personne concernée », *Dalloz IP/IT*, 2017, p. 253.

propriété soit conféré aux individus sur leurs données à caractère personnel. Envisagée comme un élément permettant aux personnes de contrôler l'utilisation de leurs données, cette patrimonialisation devrait par exemple leur permettre d'obtenir une rémunération en échange de la fourniture de données personnelles.

Ce système viserait ainsi à réduire le déséquilibre structurel entre responsables de traitement et personnes concernées, notamment car la fourniture d'un service gratuit, une application par exemple, ne serait plus suffisante pour justifier l'accès à des données nominatives. Les individus devraient également être en mesure de bénéficier de la valorisation qui est faite de leurs données à caractère personnel. Pourtant, l'idée de doter les individus d'un droit de propriété sur leurs données personnelles semble devoir être écartée. L'inadéquation des principes classiques de la propriété aux données à caractère personnel **(A)** renforcerait ainsi la perte de maîtrise de leurs informations par les individus **(B)**.

A. Inadéquation des principes classiques de la propriété

230. Le recours aux principes classiques du droit de la propriété a été envisagé pour permettre un meilleur encadrement de l'usage des données à caractère personnel dans le contexte de l'économique numérique. L'intégration des données au sein du patrimoine est apparue pour certains comme une solution qui contribuerait à renforcer la maîtrise des individus sur leurs informations nominatives[434]. Pourtant, la reconnaissance de ce droit de propriété et l'intégration des données au patrimoine des individus s'opposent à l'idée d'une protection perçue sous l'angle des droits de la personnalité et des droits fondamentaux, au sens de l'article 8 de la Charte des droits fondamentaux[435]. Le lien entre identité et propriété est ténu **(1)** et les principes classiques de la propriété ne semblent pas adaptés aux données personnelles **(2)**.

[434] Pierre Bellanger, *La souveraineté numérique*, Stock, janvier 2014, p. 201.
[435] L'article 8 de la Charte des droits fondamentaux de l'Union européenne, adoptée le 7 décembre 2000 et acquérant une valeur contraignante par l'adoption du traité de Lisbonne en 2007 dispose, « toute personne a droit à la protection des données à caractère personnel la concernant ».

1. L'absence de lien entre identité et propriété

231. Des solutions attrayantes. L'instauration d'un « droit de propriété des individus sur leurs données personnelles constitue un débat d'actualité »[436] dont la presse écrite et notamment généraliste se fait l'écho[437]. Visant à répondre de manière alternative aux questions posées par la commercialisation des données à caractère personnel, l'instauration d'un droit de propriété sur les données aurait pour but de « compenser l'activité de monétisation des données personnelles que les grandes plateformes sociales du web et les intermédiaires de données (*data brokers*) réalisent déjà »[438]. Surtout, partant du constat que « l'utilisateur ne retire aucune rémunération directe de la matière première qu'il fournit »[439], certains auteurs prônent le recours à l'institution d'un système de micro-paiement que les entreprises devraient reverser aux utilisateurs afin de pouvoir collecter, stocker et exploiter à des fins commerciales les données personnelles des utilisateurs[440]. Cette solution propose des arguments qui peuvent sembler en principe attirants, tel que le rééquilibrage des rapports de pouvoir entre les plateformes et les utilisateurs[441], mais elle n'emporte pas la conviction pour plusieurs raisons.

232. Une logique de droits attachés à la personne. Le Conseil d'Etat, dans son rapport de 2014 sur le numérique et les droits fondamentaux, rappelle qu'il n'existe « pas de droit de propriété de l'individu sur ses données personnelles » en l'état du droit. Celui-ci explique, rappelant un rapport de Pierre Truche, Jean-Paul Faugère et Patrice Flichy[442], que la protection des données personnelles, telle qu'elle est envisagée par les différents instruments nationaux et européens, ne repose pas sur une logique patrimoniale mais sur une logique de droits attachés à la personne. L'instauration d'un droit de propriété serait dès lors à même de remettre en cause la

[436] Fabrice Mattatia, Morgane Yaïche, « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? », *Lamy Droit de l'Immatériel*, n° 114, 2015, p. 60 à 63.
[437] Voir notamment : « Données personnelles et vie privée, comment reprendre le contrôle ? », Le Point, 25 janvier 2018, n° 2369.
[438] Antonio Casilli, « Quatre thèses sur la surveillance numérique de masse et la négociation de la vie privée », *Le Numérique et les droits fondamentaux*, Rapport Annuel, Conseil d'Etat, 2014, p. 423 à 434.
[439] Génération Libre, *Mes data sont à moi. Pour une patrimonialité des données personnelles*, janvier 2018, p. 8
[440] Jaron Lanier, *Who Owns the Future ?*, Simon & Schuster, New York, , 2013, 448 p.
[441] Génération Libre, *op. cit.*, p. 9.
[442] Pierre Truche, Jean-Paul Faugère, Patrice Flichy, *Administration électronique et protection des données personnelles*, La Documentation Française, février 2002, p. 110.

réglementation publique établie, puisque « la logique de marchandisation s'oppose à celle d'un droit de la personnalité placé sur le terrain de la dignité humaine »[443].

Les données personnelles, éléments relatifs à l'identité de la personne, seraient dès lors indisponibles et ne pourraient faire l'objet de commerce, en raison notamment d'une consécration récente au sein de l'article 8 de la Charte des droits fondamentaux qui fait du droit à la protection des données personnelles un droit fondamental ou, pour reprendre les termes du droit privé, un droit de la personnalité[444]. Par ailleurs, la volonté de rééquilibrage des pouvoirs entre utilisateurs et plateformes semble illusoire au regard de la valeur qu'un individu serait susceptible de dégager en exploitant lui-même et directement ses propres données personnelles. L'hypothèse de la propriété serait d'abord à même de renvoyer « à l'individu la responsabilité de gérer et protéger ses données » et surtout, « elle ne pourrait que générer des revenus anecdotiques pour les usagers »[445]. Comme l'indique le Conseil d'Etat dans son rapport en date de 2014, « même si le prix des données de chaque individu est appelé à accroître de manière considérable au cours des années à venir, la valeur de l'actif que la reconnaissance du droit de propriété conférerait à chaque individu restera dérisoire »[446]. Dès lors, les faibles revenus dégagés par les individus pour l'exploitation de leurs données personnelles ne seraient pas à même de renforcer les capacités de maîtrise des individus sur ces mêmes données et ne feraient que renforcer le déséquilibre dénoncé. Par ailleurs, conférer un droit de propriété aux individus implique que ceux-ci n'exercent pas forcément ce droit, renforçant non seulement le déséquilibre face aux entreprises du numérique, mais renforçant également les inégalités entre les personnes concernées par des traitements de données.

233. Des difficultés relatives à la nature des données personnelles. Le Conseil National du Numérique soulève par ailleurs une question relative à la nature des données personnelles. La frontière entre données personnelles et données non-

[443] Conseil National du Numérique, *Avis sur la libre circulation des données dans l'Union européenne*, avril 2017, p. 3.
[444] Gérard Cornu, *Droit civil. Les personnes*, Montchrestien, 13ème édition, Août 2007, p. 65.
[445] Conseil National du Numérique, *Rapport sur la neutralité des plateformes*, mai 2014, p. 37.
[446] Conseil d'Etat, op. cit., p. 265.

personnelles étant très fine compte tenu des « risques réels de réidentification »[447], le caractère large de la définition des données à caractère personnel rendrait l'instauration d'un droit de propriété complexe à mettre en œuvre. En effet, y procéder reviendrait à doter les individus d'un droit de propriété sur des données à caractère personnel mais également sur des données en théorie non identifiantes et donc potentiellement sur tout type de données. Les capacités de croisement et d'analyse de données non-identifiantes, l'interconnexion de données dans le cadre des objets connectés et du *quantified-self* ou encore les faiblesses relatives à certains dispositifs d'anonymisation ou de pseudonymisation seraient dès lors susceptibles de patrimonialiser un nombre important de données, plus vaste que le simple domaine des données à caractère personnel. Comme le révèle le CNNum, ce changement de paradigme risquerait par conséquent « de créer un effet domino et de concerner à terme l'ensemble des données ». La nature des données ainsi que les éléments auxquelles elles se rapportent empêchent théoriquement l'instauration d'un droit de propriété et les caractéristiques de ce dernier s'opposent également à sa mise en œuvre.

2. L'inadéquation des concepts classiques de la propriété

234. L'article 544 du Code civil définit le droit de propriété comme étant « 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 ». L'hypothèse de la propriété appliquée aux données nécessite d'analyser la compatibilité des critères classiques du droit de la propriété, traditionnellement regroupés autour des notions de l'*usus*, de l'*abusus* et du *fructus*. Instaurer un droit de propriété sur les données personnelles nécessiterait dès lors que la personne concernée par un traitement de données soit en mesure d'exercer pleinement ces éléments.

235. L'usus. Concernant d'abord l'usus, celui-ci est envisagé comme le droit « de détenir et d'utiliser une chose sans en percevoir les fruits »[448]. Droit de jouissance direct du bien, il semble directement applicable au domaine des données

[447] *Ibidem.*
[448] Raymond Guillien, Jean Vincent, *Lexique des termes juridiques*, Paris, Dalloz, 16ème édition, mai 2007, p. 666.

personnelles, comme le montrent certains auteurs. Ainsi, « lorsqu'un internaute rentre son nom et son prénom sur un site afin de s'inscrire pour pouvoir passer des commandes, il peut renseigner ses données s'il souhaite s'inscrire ou bien s'abstenir, et détient alors la faculté de décider librement de la divulgation de ses données personnelles, sans qu'il y'ait d'obligation »[449]. Une problématique serait en revanche susceptible de naître pour le cas où la propriété serait transférée. En effet, « une tierce personne acquerrait alors le droit d'utiliser des données d'autrui », ce qui serait susceptible de rendre l'usurpation d'identité légale[450].

236. Le fructus. La patrimonialisation du droit des données personnelles impliquerait également de pouvoir identifier le *fructus*, entendu comme « le droit de percevoir les fruits ». Cette composante du droit de propriété semble en réalité être déjà mise en œuvre, par la nature même des services utilisés dans le cadre de l'économie numérique. En effet, les utilisateurs ont, comme cela a déjà été mentionné précédemment, la possibilité d'avoir accès à des services en échange de leurs données à caractère personnel. Les objets connectés, en tant que produit de consommation, ne sont pas gratuitement mis à disposition des utilisateurs. Mais, en revanche, les applications utilisées dans le cadre du *quantified-self* ou encore les réseaux sociaux permettant de partager de telles données reposent sur ce système de fonctionnement et proposent donc des services en échange d'une collecte de données personnelles.

Certains opérateurs américains de téléphonie ont proposé à leurs clients d'abandonner la confidentialité de leur navigateur en échange de remise sur le montant de leur forfait annuel. En France, l'assureur Axa a offert des capteurs connectés à certains de ses clients en échange de données concernant leur activité physique[451]. Rien ne semble donc s'opposer en principe à l'identification du fructus en cas d'instauration d'un droit de propriété sur les données à caractère personnel. En effet, la jouissance étant entendu au sens de l'article 544 du Code civil comme le

[449] Fabrice Mattatia, Morgane Yaïche, « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? », *Lamy Droit de l'Immatériel*, 2015, n° 114, p. 60 à 63.
[450] *Ibid.*
[451] Elsa Bembaron, « Axa s'associe à Withings dans la santé connectée », Le Figaro, 2 juin 2014, http://www.lefigaro.fr/secteur/high-tech/2014/06/02/01007-20140602ARTFIG00239-axa-s-associe-a-withings-dans-la-sante-connectee.php

droit de faire fructifier son bien ou de le laisser improductif, un choix est donc laissé à l'individu, qui montre que celui-ci peut tout à fait rester dans l'inaction.

237. L'abusus. Les deux précédents éléments sont ceux qui soulèvent le moins de problématiques particulières. Mais le dernier critère, relatif à l'*abusus*, est en revanche susceptible de révéler l'inadéquation du régime de la propriété appliqué aux données personnelles. Ainsi, selon la doctrine civiliste, « c'est dans cet attribut que la propriété se manifeste, de façon éclatante, comme une petite souveraineté », car « le droit de disposition, de libre disposition, de disposition pleine et entière est conçu, comme le droit « d'abuser », matériellement ou juridiquement d'une chose »[452]. Or, cet aspect du droit de propriété est celui qui semble s'opposer le plus fermement à l'instauration d'une patrimonialisation des données personnelles. En effet, l'objection la plus souvent formulée tient au risque d'aliénation par l'individu de son droit de propriété par la vente de son bien et de la perte de maîtrise qui pourrait définitivement en résulter. A cet égard, « permettre à une personne de vendre ses données personnelles, sur lesquelles elle perdrait tout contrôle une fois la vente conclue, réduirait à néant sa protection »[453]. Dès lors, pour certains auteurs, la personne fichée ne serait « jamais qu'usufruitière de ses données personnelles » [454]. Les éléments relatifs à la disposition du droit de propriété ne seraient pas de nature à rééquilibrer la relation entre les individus et les entreprises, mais accentuerait au contraire cette perte de maîtrise des données par l'individu.

B. Une perte de maîtrise pour l'individu

238. La doctrine estime de manière générale que la reconnaissance d'un droit de propriété sur les données personnelles n'est pas de nature à rendre le contrôle sur ses informations à l'individu. Au contraire, cette reconnaissance « aurait pour conséquence de faire passer d'un régime de liberté réglementée de traiter des données à un régime de liberté absolue »[455]. Sans remettre en cause le recours à des éléments

[452] Gérard Cornu, *Droit civil. Les biens*, Montchrestien, 13ème édition, octobre 2007, p. 67.
[453] Anne Debet, « La protection des données personnelles, point de vue du droit privée », *Revue du Droit public*, n°1, 2016, p. 17.
[454] Nicolas 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.
[455] *Ibid.*

du droit privé permettant la mise en œuvre d'un traitement, tel que le consentement, cette solution décriée par l'ancienne présidente de la CNIL elle-même[456] présente un risque d'aliénation du droit à la protection des données des individus **(1)**, nécessitant d'écarter également l'application du droit de la propriété intellectuelle **(2)**.

1. Un risque d'aliénation du droit de propriété

239. Les difficultés d'application du concept de la propriété aux données personnelles sont concentrées autour d'obstacles de nature théorique et pratique. Le risque d'aliénation du droit de propriété réside, comme montré précédemment, dans la capacité de disposer pleinement de ses données personnelles, au sens de l'*abusus*. Ce droit de disposer des choses librement est inhérent au droit de propriété mais il aurait dans ce cas de figure vocation à s'appliquer à des données personnelles, informations relatives à l'identité de la personne. Dès lors, la reconnaissance d'un droit de propriété sur les données personnelles aurait *a fortiori* comme conséquence de permettre à l'individu de disposer pleinement d'éléments relatifs à son identité, tels que son nom, son prénom, ses caractéristiques physiques ou encore ses données sensibles telles qu'elles sont envisagées à l'article 9 du RGPD.

240. Certains auteurs, tels que Fabrice Mattatia et Morgane Yaïche, proposent d'opérer une distinction entre les données sensibles qui ne pourraient être proposées à la vente et celles moins sensibles qui pourraient être rendues disponibles à la cession ou à la location. A l'image de cette distinction, cette possibilité a été envisagée outre-Atlantique où la ligue de football américaine, concluant un accord avec une entreprise spécialisée dans le *quantified-self*, a rendu disponible à la vente les données relatives à l'effort physique, au sommeil et à la récupération de certains joueurs[457].

241. Cette distinction, bien que pertinente, ne permet pas de répondre à la question relative au pouvoir d'administration et de gestion des biens qui représente

[456] Jacques Henno, « Ceux qui pensent être propriétaires de nos données se trompent », interview d'Isabelle Falque-Pierrotin, *Les Echos*, 25 novembre 2014, https://www.lesechos.fr/25/11/2014/lesechos.fr/0203937716964_isabelle-falque-pierrotin-----ceux-qui-pensent-etre-proprietaires-de-nos-donnees-se-trompent--.htm
[457] Libby Plummer, « NFL players will soon be able to sell their own fitness data », Wired, 26 avril 2017, http://www.wired.co.uk/article/nfl-players-sell-data

« un prolongement du droit de disposer »[458]. En effet, la propriété implique pour l'individu d'administrer ses biens et cette faculté, qui représente un niveau de complexité supplémentaire dans la mise en œuvre du droit de propriété, laisse planer certains doutes quant à l'effectivité concrète d'un tel dispositif. En effet, la patrimonialisation du droit des données personnelles impliquerait pour les individus de devoir gérer leurs informations personnelles, à la manière d'un portefeuille d'actions en bourse. Les individus sont susceptibles de procéder eux-mêmes à l'administration de leurs données mais ils pourraient également en confier la charge à des entreprises spécialisées qui serviraient d'intermédiaires, à l'image de courtiers gérant des portefeuilles d'actions[459].

Le Conseil d'Etat fonde par ailleurs son refus de proposer la reconnaissance d'un droit de propriété en la matière sur la fragilisation éventuelle de toute la réglementation publique de l'utilisation des données personnelles. Certains principes fondamentaux de la réglementation s'opposent concrètement au risque d'aliénation du droit de propriété. Les articles de la LIL relatifs au droit d'accès et de rectification des données personnelles, repris en des termes similaires par le RGPD, posent la question de savoir comment un individu concerné par un traitement et qui a décidé de transférer son droit de propriété sur ses données pourrait y procéder. De manière similaire, le principe de finalité déterminé rend en pratique complexe l'instauration d'un droit de propriété et son éventuelle aliénation par le propriétaire des données. En effet, l'acquéreur ne pourra en faire l'usage que dans les limites de la finalité du traitement, déterminée en amont de celui-ci.

242. Enfin, cette faculté doit être écartée au regard de la conception européenne du droit à la protection des données personnelles. La propriété exercée sur un bien confère certaines facultés relatives à la maîtrise et à l'entretien de ce droit et la propriété est également susceptible d'être transférée, entraînant par la même occasion la transmission de l'*abusus*. Il reviendrait dès lors à un tiers de pouvoir librement disposer des données personnelles acquises et de procéder à des actes matériels de destruction ou des actes juridiques de disposition portant sur des

[458] Gérard Cornu, *op. cit.*, p. 70.

éléments relatifs à l'identité de la personne concernée initialement par un traitement de données à caractère personnel. Par ailleurs, l'article 544 avance l'idée de l'absolutisme du droit de propriété, entendu comme étant sans limites, ni restrictions. Mais le même texte indique cependant que l'exercice de ce droit est limité par l'usage « prohibé par les lois ou par les règlements », faisant de cet absolu une « prétention folle » et une « vanité » qui est « en droit positif, une illusion dérisoire »[460]. Ces différents éléments qui tendent à écarter l'idée de l'instauration d'un droit de propriété sur les données personnelles doivent également conduire à écarter l'application du droit de la propriété intellectuelle.

2. L'exclusion du droit de la propriété intellectuelle

243. La question a été posée par la doctrine de savoir si, dès lors que les entreprises exercent un droit de propriété sur les bases de données personnelles qu'elles constituent, il ne serait pas juste que les individus puissent également jouir d'un droit de propriété sur de telles bases de données[461]. A ce titre, l'hypothèse du recours au droit de la propriété intellectuelle et du droit d'auteur doit être envisagé, en raison des modalités de protection qu'ils seraient susceptibles d'apporter aux individus concernés par des traitements de données personnelles. L'adéquation de la qualification envisagée repose dès lors sur l'appréciation de la donnée personnelle au regard du Code de la propriété intellectuelle et du droit d'auteur, envisagé comme « un droit de propriété incorporelle exclusif et opposable à tous »[462] qui a vocation à s'appliquer aux œuvres de l'esprit. Le recours au droit de la propriété intellectuelle permettrait d'écarter la problématique relative à l'aliénation du droit de propriété et à la perte de maîtrise sur les données personnelles qui serait susceptible d'en résulter. En effet, le droit d'auteur présente l'avantage de mettre en œuvre des droits incessibles tels que les droits moraux et des droits cessibles tels que le droit

---

[459] Arnaud Anciaux, Joëlle Farchy, « Données personnelles et droit de propriété : quatre chantiers et un enterrement », *Revue internationale de droit économique*, 2015, n° 3, p. 307-331.
[460] Gérard Cornu, *op. cit*., p. 71.
[461] Laurent Cytermann, *op. cit*., p. 99.
[462] A ce titre, l'article L. 111-1, paragraphes 1 et 2 du Code de la propriété intellectuelle dispose que « l'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous ».

d'exploitation, cette distinction étant fondée sur le caractère purement immatériel de ce droit de propriété, « quel que soit le caractère de l'œuvre créée »[463].

244. Pour être applicable au droit de la propriété intellectuelle, les données à caractère personnel doivent cependant remplir certaines conditions. Elles doivent notamment recevoir la qualification d'œuvre de l'esprit au sens de l'article 112-2 du Code de la propriété intellectuelle. Aucune définition précise de la notion n'est donnée par l'article mais une énumération de différents supports pouvant recevoir la qualification d'œuvre de l'esprit est avancée et un critère relatif à l'originalité de l'œuvre a été déployé par la jurisprudence[464]. Faisant référence à un apport intellectuel propre et à un effort personnalisé, ces critères semblent pourtant difficiles à identifier dans le cadre de données à caractère personnel. L'apport intellectuel de l'auteur, nécessaire pour retenir cette qualification, sera difficile à établir concernant des informations relatives au nom, à l'adresse, à la géolocalisation ou encore à l'activité physique.

245. Le cas des bases de données. La question du droit de la propriété intellectuelle peut être envisagée sous l'angle des bases de données. On pourrait en effet considérer que l'ensemble des données relatives à des individus soient consignées au sein de bases dont ils auraient la gestion. La directive du 11 mars 1996 sur la protection des bases de données[465], transposée par la loi du 1er juillet 1998[466], est venue instaurer un double mécanisme de protection à l'égard des bases. La donnée n'est en l'espèce plus isolée mais elle s'insère au sein d'un ensemble cohérent de données, construit selon un raisonnement particulier. Le Code de la propriété intellectuelle vient définir la notion de base de données comme « un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen »[467]. La double protection qui est mise en œuvre s'entend d'une part de la protection des bases de données par le droit d'auteur et d'autre part d'une

[463] Gérard Cornu, *op. cit.*, p. 347.
[464] Cass., Ass. Plén., 7 mars 1986, n° 83-10477.
[465] Directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données.
[466] Loi n° 98-536 du 1er juillet 1998 portant transposition dans le code de la propriété intellectuelle de la directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données.
[467] Article L. 112-3, Code de la propriété intellectuelle.

protection *sui generis* visant à protéger spécifiquement le producteur de la base de données pour l'investissement réalisé dans la création de la base.

L'article L. 112-3 du Code de la propriété intellectuelle indique que la protection d'une base de données au titre du droit d'auteur est subordonnée à son originalité, critère qui va s'apprécier notamment par la disposition du contenu. Dès lors, le droit d'auteur viendra protéger la structure de la base et non son contenu : ce sont l'ossature de la base et les critères selon lesquels elle est agencée qui seront protégés, toute atteinte constituant dès lors un délit de contrefaçon. La base de données, si elle est protégée dans sa structure, est également protégée dans son contenu. Cette protection spécifique, dite *sui generis*, est attachée au producteur de la base. Ainsi, cette protection bénéficiera aux seuls producteurs de la base, entendus comme les personnes qui prennent « l'initiative et le risque des investissements correspondants »[468]. Le producteur de la base devra justifier de l'investissement – financier, matériel, humain – réalisé pour constituer cette base de données. Cette solution est applicable aux opérateurs du numérique, responsables de traitement, qui proposent des services. Mais l'applicabilité du dispositif aux individus semble plus complexe[469]. Ceux-ci devraient notamment réaliser les investissements nécessaires à la création de la base, en assumer les risques éventuels et surtout assurer la gestion de celle-ci. Ces différents éléments permettent de justifier l'approche actuelle, qui consacre un droit de la personnalité aux individus.

§2. La consécration d'un droit de la personnalité

246. La loi de 1978, fondement de la réglementation propre aux données personnelles, n'a pas entendu doter les individus d'un droit de propriété sur leurs données. Justifié à l'origine par la nécessité de les protéger des abus éventuels du fichage réalisé par les administrations, le texte adopté n'a pas retenu le caractère patrimonial des informations traitées. Ses caractéristiques ont d'ailleurs permis, plus tardivement, sa consécration en tant que droit fondamental. Relatives *in fine* à la

[468] Article L. 341-1, Code de la propriété intellectuelle.
[469] Célia Zolynski, « Un nouveau droit de propriété intellectuelle pour valoriser les données : le miroir aux alouettes ? », *Dalloz IP/IT*, 2018, p. 94.

protection d'informations relatives à l'identité de l'individu concerné par un traitement de données, les mesures mises en œuvre ont permis d'affirmer le caractère extra-patrimonial des données personnelles protégées **(A)**, en tant que garantie nécessaire à la maîtrise de celles-ci par l'individu **(B)**.

A. Le caractère extra-patrimonial des données personnelles

247. Dans un arrêt en date du 22 octobre 2014, la Cour de cassation, à propos d'une condamnation pour abus de confiance, a confirmé la nature juridique des données, entendues comme des biens au sens de l'article 314-1 du Code pénal[470]. L'application de cette qualification au cas spécifique des données personnelles doit cependant être écartée, en raison notamment des spécificités du régime traditionnel de la propriété civile cristallisée autour de la notion de patrimoine. Par définitions indisponibles car ne pouvant être vendues, les données à caractère personnel sont donc des biens inaliénables **(1)** et insaisissables **(2)**.

1. Un bien inaliénable

248. Comme le révèle le Conseil d'Etat dans son rapport en date de 2014, plusieurs éléments s'opposent à la patrimonialisation des données à caractère personnel. Le principe de finalité déterminée, par exemple, « est ce qui fait que les données personnelles ne sont pas des marchandises ou, du moins, qu'elles ne sont pas des marchandises comme les autres »[471]. En effet, celles-ci peuvent faire l'objet de transferts et de différentes opérations regroupées sous l'appellation de traitement mais, « le droit de propriété de leur acquéreur reste limité par les droits de la personne sur ses données »[472]. Ces droits de la personne empêchent la reconnaissance d'un droit de propriété sur une donnée brute et ce en dépit du support durable et transmissible par laquelle elle est matérialisée.

249. Les droits de la personnalité, inhérents à la personne humaine, ne peuvent faire l'objet d'atteintes et sont protégés à ce titre. Par ailleurs, en matière de données

[470] Cass. Crim, 22 octobre 2014, n° 13-82.630.
[471] Conseil d'Etat, *op. cit.*, p. 172.
[472] *Ibid.*

à caractère personnel, « c'est moins le concept d'information qui importe que les actions dont elle peut être l'objet »[473]. Dès lors, les informations relatives aux individus concernés par des traitements, relatives à des éléments de la personnalité et de l'identité, seraient des biens immatériels hors du commerce, non susceptibles d'être cédés. Outre le caractère fondamental des droits associés à la protection des données personnelles et qui découlent, entre autres, du lien établi entre vie privée et protection des données à caractère personnel, les données en elles-mêmes ne pourraient faire l'objet d'une éventuelle cession[474].

250. Le cas des licences. Certaines positions doctrinales, constatant que « les enjeux de la commercialisation des données peuvent être un frein à l'engagement des socionautes », invitent à envisager d'autres pistes de qualification juridique qui pourraient s'inspirer « du régime juridique des communs » afin notamment de rendre ces données inaliénables[475]. Le but affiché serait de permettre une protection collective des données à caractère personnel, invitant à en repenser les modalités d'usage et de réutilisation[476]. Des solutions similaires existent déjà, à l'image des modalités de mise à disposition et de réutilisation qui sont mises en œuvre dans le cadre du projet *Creative Commons* qui permet, par divers types de licences[477], de mettre différentes catégories d'œuvres numériques à la disposition du public[478].

Les licences proposées impliquent par exemple de mentionner qui est à l'origine de la création du contenu, si une utilisation commerciale est prévue ou non et si elle est soumise à l'autorisation du créateur du contenu. Cette solution, proche de celle retenue par le droit de la propriété intellectuelle, se différencie « en revanche de la règlementation concernant le domaine public, l'ayant droit pouvant choisir entre plusieurs niveaux d'autorisation et conservant l'ensemble de ses droits moraux de propriété intellectuelle »[479]. L'hypothèse consistant à faire des données personnelles

[473] Jean-Christophe Galloux, « Ebauche d'une définition juridique de l'information », *Recueil Dalloz*, 1994, p. 229.
[474] CEDH, grande chambre, *S. et Marper c. Royaume Uni*, 4 décembre 2008.
[475] Gérard Aschieri, Agnès Popelin, *Réseaux sociaux numériques : comment renforcer l'engagement citoyen ?*, Les avis du CESE, Les éditions des Journaux Officiels, janvier 2017, p. 30.
[476] Eugeny Morozov, *To Save everything, click here : the folly of technological solutionism*, Hachette UK, mars 2013, p. 36.
[477] Voir notamment : Lionel Maurel, « Données personnelles et communs : une cartographie des thèses en présence », *S.I. Lex*, 15 novembre 2017, accessible en ligne à cette adresse : https://scinfolex.com/2017/11/15/donnees-personnelles-et-communs-une-cartographie-des-theses-en-presence/
[478] Mélanie Dulong de Rosnay, « Données ouvertes (*Open Data*) », *in* Marie Cornu, Fabienne Orsi, Judith Rochfeld (dir.), *Dictionnaire des biens communs*, PUF, 2017.
[479] Thomas Giraud, « Les licences Creative Commons, une culture du partage », *JAC*, 2014, n°10, p.36.

des *commons* réutilisables est néanmoins subordonnée à l'idée d'une reconnaissance préalable de droits moraux sur les contenus créés. Surtout, la mise en œuvre de telles licences impliquerait pour l'individu un pouvoir de gestion qui, au vu de la quantité de données personnelles créées par un même utilisateur dans le cadre de l'automesure, rendrait difficile l'application pratique d'une telle approche.

251. L'instauration d'une redevance. L'instauration d'une redevance, à l'image de celle mise en œuvre pour les cas de réutilisation d'informations de nature publique dans le cadre de l'*open data*, pourrait également être mise en œuvre. Il s'agirait ainsi de soumettre les modalités de réutilisation des données personnelles des individus au versement d'une certaine somme d'argent. L'article 15 de l'ancienne loi CADA relative à la transparence de l'action publique indiquait ainsi que la réutilisation « pouvait donner lieu au versement d'une redevance » [480]. Cette solution, fondée sur le versement d'une somme d'argent en échange de la réutilisation par les entreprises du numérique des données personnelles qu'elles collectent, aurait pour avantage de ne pas procéder à un éventuel transfert de propriété de telles données.

Pourtant, cette solution - déjà conceptualisée aux Etats-Unis[481] - ne permettrait pas véritablement de garantir aux individus une meilleure maîtrise de leurs données personnelles. L'utilisateur, en contrepartie de la mise à disposition d'un pack de données, est rémunéré par l'attribution de dividendes. Aucune garantie ne lui est cependant apportée quant aux modalités de réutilisation des données à caractère personnel mises à disposition. La comparaison avec le régime juridique relatif à l'ouverture des données publiques est cependant limitée, la loi du 28 décembre 2015 ayant notamment fait de la gratuité de la réutilisation des informations le principe par défaut[482]. Ainsi, outre leur inaliénabilité, les données à caractère personnel se présentent également comme des biens insaisissables mais aussi incessibles.

[480] Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.
[481] Kenneth C. Laudon, « Markets and privacy », *Communications of the ACM*, vol. 39, n°9, 1996, p. 92 à 104.
[482] Loi n° 2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public, JORF n°0301 du 29 décembre 2015.

2. Un bien insaisissable et incessible

252. Selon la classification traditionnelle des éléments du patrimoine, tous les éléments le composant relèvent soit de l'actif, soit du passif selon la distinction de l'avoir et du devoir[483]. Dès lors, le patrimoine de l'individu englobe les biens en théorie appréciables en argent mais il regroupe également les dettes d'une personne et donc ses obligations monétaires. Saisissabilité et cessibilité des éléments du patrimoine font donc partie de ces caractéristiques. Une créance peut ainsi être cédée à un tiers et un créancier pourra, à l'inverse, saisir les biens du débiteur ou les faire vendre pour recouvrir sa créance sur le prix de vente. Ces aspects classiques de la propriété ne pourraient que difficilement s'appliquer au cas des données à caractère personnel.

253. Les données, en cas de patrimonialisation, pourraient être grevées de créances. Des tiers pourraient dès lors théoriquement faire saisir des données à caractère personnel d'un individu afin de recouvrir leurs dettes ou pourraient les faire vendre judiciairement pour être en mesure de se payer sur le prix de vente.

Une telle solution semble difficilement concevable en pratique. Il semble en effet inconcevable de pouvoir faire vendre les données relatives au nom, au prénom ou encore à l'orientation sexuelle ou à l'activité physique pour faire cesser la dette du débiteur, personne concernée à l'origine par un traitement de données. Ces informations, relatives à l'état de la personne, concerne également son identité. Or celle-ci est conçu « comme le sujet d'une dignité qui oblige à la traiter comme une fin en soi, à la différence de la chose qui peut être instrumentalisée, en considération de son utilité, comme un simple moyen »[484].

254. Une exception liée à la mort numérique. Le droit à la protection des données à caractère personnel est perçu comme un droit fondamental empêchant toute instauration d'un droit de propriété sur de telles données. On note cependant une certaine inflexion quant à l'incessibilité de telles données et des droits qui y sont afférents. La loi pour une République numérique a été amenée à traiter de la question

[483] Gérard Cornu, *op. cit.*, p. 9.
[484] Grégoire Loiseau, « Typologie des choses hors du commerce », *RTD Civ.*, 2000, p. 47.

de la mort numérique et du devenir des données personnelles de la personne décédée. Elle n'a pas eu pour objectif d'instaurer une véritable dévolution successorale des données personnelles au profit des héritiers. Cependant, l'article 63 de cette loi a été inséré au sein de la LIL et précise que si « les droits ouverts à la présente section s'éteignent au décès de leur titulaire », ceux-ci peuvent sous certaines conditions « être provisoirement maintenus ». Cette disposition a pour objectif de permettre à la personne concernée par un traitement de données de définir à l'avance le sort de ses données après son décès. Selon la loi, toute personne peut donc définir des directives générales ou particulières relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès. Ce sont ainsi les héritiers qui auront qualité, sauf directives contraires de la part de la personne concernée par le traitement, pour prendre connaissance des directives au décès de leur auteur et demander leur mise en œuvre aux responsables de traitement concernés. Ces dispositions n'ont pas pour effet de rendre transmissibles les données à caractère personnel à cause de mort. Mais elles ont pour objectif de permettre à une personne concernée par un traitement de données de déterminer à l'avance l'usage qui sera fait des données après sa mort. Cette disposition s'inscrit dans un mouvement plus général de maîtrise, par les individus, des données à caractère personnel les concernant.

B. La maîtrise de ses données personnelles par l'individu

255. L'exclusion des considérations relatives à l'instauration d'un droit de propriété des individus sur leurs données à caractère personnel doit contribuer à garantir une certaine autodétermination informationnelle aux utilisateurs de services numériques. Les individus doivent ainsi disposer de la capacité à décider pleinement et en pleine conscience de la communication et de l'utilisation des données les concernant. La reconnaissance effective d'un tel droit mettrait en œuvre « une grille de lecture nouvelle en France du droit à la protection des données personnelles » [485] et lui conférerait un contenu positif. C'est à terme l'*empowerment* des individus sur

[485] Jean-Philippe Foegle, « Le Conseil d'Etat, héraut de la révolution numérique ? », La Revue des droits de l'homme, [En ligne], Actualités Droits-Libertés, mis en ligne : 30 décembre 2014, consulté le 15 janvier 2016. URL : http://revdh.revues.org/1038.

leurs données qui est envisagé **(1)**, à l'heure ou des leviers d'action collectifs sont mis en place **(2)**.

1. La notion d'*empowerment*

256. La notion d'*empowerment* ou « empouvoirement » fait référence à la souveraineté exercée par les individus sur leurs données, dans une société qui repose de plus en plus sur l'utilisation de services numériques, sur l'interconnexion des dispositifs et le croisement de données[486]. Cette notion découle directement de celle d'autodétermination informationnelle identifiée dès 1983 par la Cour constitutionnelle fédérale d'Allemagne, réceptionnée par la jurisprudence de la CEDH : cette dernière a ainsi considéré que « l'essence même de la protection des données est de régir l'usage fait des données personnelles et ainsi de protéger ce que la Cour constitutionnelle fédérale allemande a appelé le droit à l'autodétermination informationnelle »[487]. Un tel droit s'inscrit dans la logique « du principe de la dignité de la personne humaine » en ce qu'il implique d'une part « la liberté de la personne humaine à exercer effectivement son libre-arbitre » et d'autre part, le fait que « ce soit l'individu lui-même qui définisse les conditions de base de son identité et de son parcours de vie »[488]. Un tel droit serait donc lié à celui du respect de la personnalité[489].

257. Le phénomène de « dissémination consciente ou inconsciente des données personnelles », évidemment mis en œuvre par le déploiement massif d'objets connectés, nécessite pour certains « de poser davantage la question de la renonciation de chacun à son droit au respect de sa vie privée, de sa portée, de ses modalités et de ses limites »[490]. Le droit à l'autodétermination informationnelle vise justement à répondre à cette question en replaçant l'individu au cœur du dispositif et en le dotant de moyens d'actions permettant d'assurer concrètement ses droits et permettant

---

[486] Pierre Bellanger, « De la souveraineté numérique », *Le Débat*, vol. 170, n° 3, 2012, p. 149 à 159.
[487] CEDH, gde ch., affaire *Magyar Helsinki Bizottsàg c. Hongrie*, 8 novembre 2016, 18030/11.
[488] Nicolas Ochoa, « Précisions sur l'article 9 de la loi du 06 janvier 1978 (CE, 11 mai 2015), *Les Petites Affiches*, 7 sept. 2015, n°178, p. 7.
[489] Michel Fromont, « Jurisprudence constitutionnelle de la République fédérale d'Allemagne (2008) », *Revue du Droit public*, novembre 2009, n°6, p. 1721.
[490] Didier 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*, juin 2015, n° 48, p. 35.

« d'affirmer la primauté de la personne qui doit être en mesure d'exercer sa liberté »[491]. La CNIL rappelle à cet égard qu'il ne s'agit pas de doter l'individu de droits illimités sur ses données à caractère personnel, notamment concernant les traitements réalisés dans le cadre de missions de service public ou dans l'intérêt général. Mais un tel droit doit venir renforcer les principes déjà proclamés afin de les irriguer, de les diriger et de leur donner un but précis et convergeant de manière générale vers la maîtrise par l'individu de ses données[492].

La reconnaissance générale d'un droit à l'autodétermination informationnelle est pourtant susceptible de soulever des questions pratiques, relatives notamment au nombre élevé d'interlocuteurs auxquels les individus sont susceptibles d'être confrontés et auprès desquels ce droit à l'autodétermination devrait être effectivement appliqué[493]. La diversité des opérateurs appelés à intervenir pour un même traitement de données, tel que c'est le cas pour les objets connectés, pourrait ainsi vider ce droit de toute possibilité d'application concrète[494].

258. A ce titre, le droit à la portabilité des données[495] s'inscrit parmi les nouvelles mesures permettant la traduction concrète et la mise en œuvre effective du droit à l'autodétermination informationnelle, tel qu'il est désormais inscrit à l'article premier de la loi Informatique et Libertés de 1978. Ce droit à la portabilité doit permettre à un individu d'avoir accès à ses données personnelles afin de pouvoir les récupérer et les transférer vers un autre service qui lui serait plus adapté. En matière d'objets connectés et de *quantified-self*, on peut envisager l'hypothèse de l'individu ayant accès à ses données de bien-être (sommeil, marche, course à pieds, poids) afin de les récupérer et de les transférer vers un autre dispositif mieux adapté à ses besoins. En permettant à l'individu de décider de l'usage qui est fait de ses données, « la portabilité participe enfin de son autodétermination informationnelle »[496]. Le considérant 68 du RGPD retient cette conception pour les personnes concernées par

[491] Jacky Richard, « Le numérique et les données personnelles : quels risques ? quelles potentialités ? », *Revue du droit public*, janvier 2016, n°1, p. 87.
[492] CNIL, Délibération n° 2015-414 portant avis sur un projet de loi pour une République numérique, 19 novembre 2015.
[493] Juliette Sénéchal, « La diversité des services fournis par les plates-formes en ligne et la spécificité de leur rémunération, un double défi pour le droit des contrats », *AJCA*, 2016, p.141.
[494] Autorité de la concurrence, *Note sur le projet de loi pour une République numérique*, 10 novembre 2015, p. 8.
[495] Cf., *infra*, n° 327.
[496] Charly Berthet, Célia Zolynski, Nicolas Anciaux, Philippe Pucheral, *op. cit.*, p. 29.

des traitements et il indique que cette mesure doit « renforcer encore le contrôle qu'elles exercent sur leurs propres données ».

Pourtant, le lien entre droit à la portabilité et autodétermination informationnelle doit être tempéré[497]. En effet, il semble « davantage reconnu dans une perspective commerciale et concurrentielle que dans une perspective de protection de la vie privée de l'individu »[498] et celui-ci ne permettrait pas d'assurer concrètement la maîtrise par les individus de leurs données à caractère personnel. Le rééquilibrage des rapports entre entreprises du numérique et individus est primordial pour l'exercice concret du droit à l'autodétermination. Il doit éviter aux individus d'être placés dans une situation de déséquilibre face aux responsables de traitement, les empêchant de pouvoir agir concrètement pour la maîtrise de leurs informations. La mise en œuvre d'une action de groupe est apparue être une solution permettant de procéder à ce rééquilibrage.

2. La création de leviers d'action collectifs

259. Les individus concernés par des traitements de données personnelles sont souvent perçus comme étant dans une situation défavorable au regard du poids économique des acteurs du numérique. Les objets connectés utilisés pour la pratique du *quantified-self* sont des instruments parfois développés par de jeunes entreprises aux capacités financières limitées. Mais ceux-ci sont généralement le produit de grandes entreprises du numérique, généralement regroupées sous l'appellation GAFA ou GAFAM (*Google*, *Apple*, *Facebook*, *Amazon*, *Microsoft*). Or, celles-ci ont des moyens d'action juridiques et financiers importants qui placent les individus dans une situation de dépendance et les empêchent parfois de disposer de moyens d'action juridiques efficaces.

260. Un rééquilibrage des moyens d'action. La création d'une action de groupe a ainsi été envisagée, afin de permettre un rééquilibrage des moyens d'action entre individus et fournisseurs de service, conférant la possibilité à plusieurs

[497] Cf., *infra*, n° 330.
[498] Nathalie Martial-Braz, « Les nouveaux droits des individus consacrés par la loi pour une République numérique. Quelles innovations ? Quelle articulation avec le Règlement européen ? », *Dalloz IP/IT*, 2016, p. 525.

individus de regrouper leurs moyens d'action. Cette action n'était pas envisagée dans la rédaction initiale de la loi Informatique et Libertés. Mais l'étendue des moyens de traitement employés par les entreprises du numérique a justifié que des individus, subissant des atteintes similaires, puissent s'unir pour obtenir réparation de leur préjudice ; cette faculté a été introduite avec l'adoption de la loi de modernisation de la justice du 21ème siècle[499].

Un cadre général à l'action de groupe devant les juges judiciaires et administratifs a été déterminé[500] et sa transposition au domaine des données à caractère personnel a été effectuée à l'article 37 de la LIL qui dispose, en substance, que « lorsque plusieurs personnes physiques placées dans une situation similaire subissent un dommage ayant pour cause commune un manquement de même nature aux dispositions du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi […], une action de groupe peut être exercée devant la juridiction civile ou la juridiction administrative compétente ». Cette disposition permet de dévoiler les conditions cumulatives permettant la mise en œuvre de l'action de groupe et ses finalités, strictement encadrées, ont évolué pour permettre, outre la cessation du manquement, la réparation des préjudices matériels et moraux subis[501].

261. Un rééquilibrage limité. Le spectre de cette action de groupe est limité par la loi puisque celle-ci indique dans un point IV de l'article 37 que seules peuvent exercer cette action de groupe certaines associations ayant pour « objet statutaire » la protection « de la vie privée et la protection des données à caractère personnel » ou encore « les associations de défense des consommateurs […] lorsque le traitement de données à caractère personnel affecte des consommateurs » et enfin « les organisations syndicales de salariés ou de fonctionnaires » lorsque « le traitement affecte les intérêts des personnes que les statuts de ces organisations les chargent de défendre ».

[499] Loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIème siècle, JORF du 19 novembre 2016.
[500] Caroline Fleuriot, « L'action de groupe s'ouvre à de nouveaux domaines », *Dalloz Actualité*, 22 novembre 2016.
[501] La loi Informatique et Libertés, avant sa réécriture par l'ordonnance du 12 décembre 2018, indiquait simplement que l'action de groupe avait pour objectif la cessation du manquement. Le RGPD, en son article 80, est venu préciser que l'action de groupe susceptible d'être déclenchée pouvait avoir pour but la réparation d'un éventuel dommage subi par la personne concernée par un traitement de données à caractère personnel.

L'action de groupe, outre le renforcement des capacités d'action qu'elle est censée conférer aux utilisateurs de services numériques, peut également être appréciée au regard de son caractère dissuasif pour les entreprises, en raison des sanctions économiques et réputationnelles auxquelles elles sont exposées[502]. Dès lors, « c'est à leur fonction dissuasive et non réparatrice que doit être jugée l'efficacité des actions de groupe ». Cependant, la portée dissuasive de l'action de groupe doit être tempérée, la publicité et le montant des sanctions prononcées jouant déjà ce rôle. Par ailleurs, même si les actions de groupe ont aujourd'hui tendance à se développer, leurs conditions strictes de mise en œuvre, déjà modifiées par l'adoption de la loi du 20 juin 2018[503], sont susceptibles d'affaiblir la pertinence du dispositif[504]. Dès lors, celles-ci ne permettraient pas de limiter *ex ante* l'asymétrie informationnelle mise en œuvre dans le cadre de l'utilisation de services du numérique.

SECTION II. UNE ASYMÉTRIE INFORMATIONNELLE RENOUVELÉE

262. Le cadre juridique relatif à la protection des données personnelles est fragilisé par des éléments de nature variée, liés à la croissance exponentielle des moyens de traitement mis en œuvre. Cette fragilisation s'articule de plus en plus autour de la notion d'asymétrie informationnelle, censée illustrer le déséquilibre dans les rapports existants entre fournisseurs de services à l'ère du numérique et utilisateurs de ces mêmes services. Parfois rapprochée de la notion de loyauté des plateformes[505] auquel elle s'oppose, la question de l'asymétrie informationnelle est en tout cas marquée par les difficultés, pour les responsables de traitement, à communiquer de manière transparente sur les pratiques qui sont mises en œuvre.

L'asymétrie informationnelle est renforcée par « l'ignorance des usagers quant aux codes de fonctionnement des systèmes mis à l'œuvre derrière leurs usages » et

[502] Emmanuelle Claudel, « Action de groupe et autres dispositions concurrence de la loi consommation : un dispositif singulier », *RTD com.*, 2014, p. 339.
[503] LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.
[504] Xavier Gabaix, Augustin Landier, David Thesmar, *La protection du consommateur : rationalité limitée et régulation*, Conseil d'Analyse Economique, La documentation française, 2013, p. 42.
[505] Judith Rochfeld, Célia Zolynski, « La « loyauté » des « plateformes ». Quelles plateformes ? Quelle loyauté ? », *Dalloz IP/IT*, 2016, p. 520.

qui leurs sont proposés[506]. Ainsi, « la sphère marchande entretient en effet l'usager dans un univers spécifique, comme une forme d'enfermement qui ne serait pas tangible »[507]. L'asymétrie informationnelle, renforcée par cette opacité, a pour effet de déséquilibrer les relations marchandes **(§1)** et de fausser, dans certains cas, le consentement des personnes concernées par des traitements de données à caractère personnel **(§2)**.

§1. Une relation commerciale déséquilibrée

263. Les instruments de protection des données à caractère personnel reposent tous sur un système selon lequel le traitement des données personnelles est en théorie libre. La personne concernée par le traitement doit simplement avoir été en mesure de donner son consentement – libre, spécifique, éclairé et univoque[508] – à la réalisation d'une telle opération et ce en vertu d'une information claire et complète délivrée par le responsable de traitement[509]. Déjà mobilisés par la directive 95/46/CE, ces éléments sont renouvelés par le RGPD qui renforce le devoir d'information et permet une appréhension renouvelée du consentement des individus, manifesté par une déclaration ou un acte positif clair.

L'asymétrie informationnelle remet pourtant en question ces différents instruments et influence aujourd'hui les différentes composantes du consentement, en raison de la nature même des services qui sont mis en œuvre et qui ont pour effet de plonger la régulation « dans une sorte de situation d'impuissance structurelle »[510]. Les nouveaux outils technologiques qui sont aujourd'hui largement utilisés ne font qu'amplifier ce risque d'asymétrie informationnelle, en raison notamment du développement d'une économie « behavioriste » **(A)** conférant une valeur marchande aux données collectées par les fournisseurs de services numériques **(B)**.

---

[506] Bénédicte Rey, « Les intelligences numériques des informations personnelles. Vers un changement de perspective pour garantir le droit à la vie privée ? », *Les Cahiers du numérique*, 2014/1, Vol. 10, p. 9 à 18.
[507] *Ibid.*
[508] Article 4, Règlement (UE) 2016/679.
[509] Article 13, Règlement (UE) 2016/679.
[510] Alain Rallet, Alain, Fabrice Rochelandet, « La régulation des données personnelles face au web relationnel : une voie sans issue ? », *Réseaux*, n°3, 2011, p. 17 à 47.

A. Le développement d'une économie « behavioriste »

264. Les entreprises proposant des services de *quantified-self* ont tendance à collecter de plus en plus de données relatives à leurs clients afin de proposer des services toujours plus personnalisés. Celle collecte massive de données est rendue nécessaire par l'émergence d'une économie fondée sur la connaissance du client et sur le développement d'outils marketing ciblés. La valeur d'usage de l'offre de services en ligne va dépendre de la « production de données par les individus eux-mêmes »[511] et cette production est impactée par la multiplication des moyens de collecte. Un véritable web-symbiotic va se déployer **(1)**, dans lequel l'échange constant de données à caractère personnel va révéler le paradoxe relatif aujourd'hui à la vie privée **(2)**.

1. Web-symbiotic et logique de valorisation des données

265. L'exigence d'un consentement libre. Le consentement de l'individu, requis pour procéder au traitement de données à caractère personnel, doit présenter certaines caractéristiques précises. Celui-ci, pour être valable, doit d'abord être libre. L'article 7, paragraphe 4, du RGPD permet de donner des éléments d'appréciation quant à ce critère et indique qu'il y'a lieu, au moment de déterminer si le consentement est donné librement, 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 ». Cette disposition a vocation à empêcher que la fourniture d'un service soit conditionnée par la collecte de données qui ne sont pas nécessaires à son exécution. Le G29, par référence à la « conditionnalité », considère « que le consentement au traitement de données à caractère personnel non nécessaires ne peut pas être considéré comme une condition *sine qua non* de l'exécution d'un contrat ou de la fourniture d'un service »[512].

[511] Grazia Cecere, Fabrice Le Guel, Fabrice Rochelandet, « Les modèles d'affaires numériques sont-ils trop indiscrets ? Une analyse empirique », *Réseaux*, n° 189, 2015, p. 77 à 101.
[512] G29, *Lignes directrices sur le consentement au sens du règlement 2016/679*, WP259, adoptées le 28 novembre 2017, version révisée et adoptée le 10 avril 2018.

266. Un consentement conditionné. Cette liberté du consentement fait pourtant l'objet d'un certain nombre de remises en question. Selon une formule maintenant largement répandue, « lorsqu'un service ou un bien est proposé gracieusement à un individu, c'est l'individu – ou plus exactement ses données – qui constituent la valeur marchande »[513]. Le concept de *web-symbiotic* a été mobilisé par certains auteurs pour faire référence à l'échange constant de données à caractère personnel ayant lieu entre fournisseurs de services numériques et individus[514]. Dès lors, une nouvelle forme de symbiose se mettrait en place entre internautes d'une part et entreprises de l'autre, chacune de ces entités devenant dépendantes l'une de l'autre dans le contexte actuel de l'économie numérique. Celle-ci établit un modèle qui repose justement sur la conditionnalité du consentement et sur une divulgation volontaire de données personnelles par les individus en échange de services et de contenus, remettant en cause le lien direct et objectif qui doit exister entre le traitement des données et l'objectif d'exécution du contrat[515].

Les réseaux sociaux ainsi que les moteurs de recherche ont été parmi les premiers à mettre en œuvre ce lien, les individus pouvant avoir accès à des services en contrepartie de la fourniture de données personnelles appelées à être monétisées par ces sociétés. Dans ce cas de figure, l'exploitation des données personnelles présente des avantages réciproques puisque chacune des parties en présence en tire un bénéfice direct. D'un côté, les internautes ont accès à un service alors que de l'autre, les entreprises ont accès aux données personnelles qu'elles peuvent exploiter pour pouvoir éventuellement développer de nouveaux services complémentaires en lien avec leur activité. Un modèle économique similaire est déployé par les objets connectés utilisés pour la pratique de l'automesure. Ceux-ci, payants, fonctionnent avec des applications qui sont généralement gratuites et dont le développement et le fonctionnement reposent dès lors sur l'exploitation de données à caractère personnel.

---

[513] Noémie Weinbaum, « Les données personnelles confrontées aux objets connectés », *Communication Commerce électronique*, n°12, décembre 2014.
[514] Paul Bernal, « Web 2.5: the symbiotic web », *International review of Law, Computers & Technology*, n° 24/1, 2010, pp. 25-37.
[515] G29, *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*, WP 217, adopté le 9 avril 2014, p. 18.

267. Une disparition apparente du prix. Comme le révèle la doctrine, il est possible de noter « la tendance à la disparition du prix dans nombre de contrats s'opérant sur Internet, créant, ce faisant, dans l'esprit des internautes le sentiment erroné qu'Internet est un espace de gratuité dès lors que les échanges économiques qu'ils réalisent ne semblent en apparence pas faire l'objet d'une rémunération »[516]. Ce mécanisme de valorisation des données personnelles mis en œuvre, qu'il repose ou non sur la publicité ciblée, a pour objet les données qui sont transmises de manière directe par l'internaute lors de l'utilisation des services. Mais il peut également porter sur des données dites passives que les individus n'ont pas conscience de créer en utilisant un service. Ces métadonnées ne sont pas toujours identifiantes mais elles peuvent également être valorisées par les entreprises du numérique.

268. Des difficultés liées au nombre d'opérateurs. Les objets connectés mettent en œuvre une chaîne de traitements de données personnelles qui fait intervenir plusieurs responsables de traitements ou plusieurs sous-traitants. Cette architecture décentralisée contribue également à renforcer le déploiement d'une asymétrie informationnelle. Dans un cas, les objets connectés jouent le rôle de « canal étroit » par lequel un service est fourni en échange d'une rémunération. Dans d'autres cas, en revanche, ils représentent « un canal beaucoup plus large *via* lequel de multiples applications, contenus numériques et services vont pouvoir être mis en œuvre »[517]. Dans la première hypothèse, l'individu n'a qu'un seul interlocuteur mais il est confronté dans le second cas à un nombre important d'opérateurs appelés à traiter des données à caractère personnel. Cette multiplication d'interlocuteurs renforce l'idée d'une perte de maîtrise des informations divulguées, sans pouvoir parfois en mesurer la portée lorsque des données dites passives sont également collectées.

Ce type de situation a de plus en plus vocation à être encadré par la réglementation[518]. Mais, la multiplication exponentielle des différents acteurs qui interviennent dans les traitements de données est source de manque de visibilité pour

[516] Juliette Sénéchal, « La fourniture de données personnelles par le client via Internet, un objet contractuel ? », *AJ Contrats d'affaires – Concurrence – Distribution*, 2015, p. 212.
[517] *Ibidem*.
[518] Cf., *supra*, n° 103.

la personne concernée qui n'a pas toujours accès à une information détaillée et peut dès lors perdre la maîtrise de ses informations identifiantes en consentant à des traitements portant sur des données qui ne sont pas nécessaires à l'exécution du service qui lui est fourni. Surtout, cette logique d'asymétrie informationnelle entre d'une part, acteurs du numériques appelés à exploiter des données et d'autre part, individus ayant vocation à utiliser des services, est à l'heure actuelle renforcée par le phénomène du paradoxe de la vie privée qui contribue à la généralisation des services reposant sur un consentement conditionné.

2. Le paradoxe de la vie privée

269. Une opposition entre protection et divulgation. Le paradoxe de la vie privée est un concept qui a été mobilisé pour exprimer la discordance qui existe entre l'affirmation des principes de protection d'un côté et les pratiques réelles de divulgation par les individus de l'autre. Cette expression est employée pour montrer la dichotomie qui existe donc entre l'inquiétude des individus quant à la diffusion de leurs données et le fait qu'ils ne modifient pas leurs comportements sur les réseaux numériques. Au contraire, ceux-ci ont tendance à dévoiler de plus en plus d'informations nominatives et relatives à leur vie privée. Dès lors, ce paradoxe serait susceptible de « transformer les citoyens en individus schizophrènes », en même temps qu'il délégitimerait « le combat pour la protection des données personnelles »[519]. Par ailleurs, ce paradoxe de la vie privée, profitant aux entreprises proposant des services fondés sur la connaissance de ses clients[520], fait que ce sont les individus qui deviennent directement créateurs des risques pesant sur leurs données personnelles.

Conceptualisé à l'origine à partir de l'observation des comportements des internautes sur les réseaux sociaux[521], le paradoxe de la vie privée expliquerait en partie aujourd'hui les difficultés à mettre en œuvre une réglementation protectrice des

[519] Antony Emorine, « Les données personnelles des français protégées par les autorités irlandaises, allemandes et luxembourgeoises : l'Europe des droits numériques en marche ... sans la Commission », *Les Petites Affiches*, n°245, 9 décembre 2015, p. 7.
[520] Patricia A. Norberg, Daniel R. Horne, David A. Horne, « The privacy paradox : personal information disclosure intentions versus behaviors », *Journal of Consumer Affairs*, Volume 41, Issue 1, march 2007, pp. 100-126.

données personnelles efficace. En effet, comment protéger efficacement des données personnelles que les individus divulguent de manière volontaire, alors que ceux-ci utilisent de plus en plus de services permettant un croisement et une interconnexion de données dont ils n'ont pas toujours conscience ? La pratique de l'automesure renouvelle aujourd'hui ces problématiques relatives au *privacy paradox*. Les craintes des internautes concernant leur vie privée et leur identité numérique ont été à l'origine exacerbées par les révélations d'Edward Snowden sur la surveillance réalisée par la NSA[522]. Mais celles-ci sont aujourd'hui renouvelées par le développement et l'utilisation croissante d'objets connectés porteurs de risques de dissémination de données[523]. La protection de la vie privée des individus serait donc précarisée par des données qui sont créées aussi bien directement qu'indirectement par l'utilisation des services proposés[524].

270. Un changement de paradigme. Dans le cadre du *quantified-self*, le paradoxe de la vie privée est à mettre en lien avec le fait que l'on assiste à un changement de paradigme. L'accession à certains services est conditionnée par la révélation de la vie privée des individus. Dès lors, le principe du *quantified-self* relève d'une exposition constante de soi et d'éléments relatifs à la vie privée ou encore à l'intimité corporelle d'un individu. A ce titre, et dans le prolongement de ce qui est identifié à travers la notion de web *symbiotic*, la divulgation de données personnelles devient une condition nécessaire à l'existence du service lui-même[525]. Outre la relation de dépendance propre aux services numériques, le paradoxe de la vie privée est conditionné par la mise à disposition gratuite de services toujours plus innovants par les entreprises du numérique, qui représentent autant de plateformes d'exposition pour les individus.

---

[521] Susan B. Barnes, « A privacy paradox : Social networking in the United States », *First Monday*, Volume 11, Number 9, 4 September 2006.
[522] David Lyon, *Surveillance After Snowden*, Polity Press, 2015, p. 15.
[523] Geoff Mulligan, « The internet of things : here now and coming soon », *IEEE Internet Computing*, 2010, vol. 14, n° 1, p. 35.
[524] Michael J. Corby, « The case for privacy », *Information Systems Security*, 2002, vol. 11, n° 2, p. 9.
[525] Sara M. Watson, « Living with Data : Personal Data Uses of the Quantified Self », *Oxford Internet Institute*, Masters Thesis, 2013, p. 9.

271. Une absence de choix. Le principe du consentement libre implique que les personnes concernées disposent d'un véritable choix entre un service incluant le consentement à l'utilisation de données à caractère personnel à des fins complémentaires et un service équivalent proposé par le même responsable du traitement n'impliquant pas de consentir au traitement de données à d'autres fins[526]. Pourtant, en vertu du paradoxe de la vie privée, les individus ne seraient pas en mesure de faire un véritable choix, notamment car les avantages offerts par des services en ligne « peuvent être considérés comme supérieurs aux inconvénients générés par la logique commerciale qui rend possible leur gratuité » [527]. Une personne préférera par exemple recevoir de la publicité ciblée plutôt que de se passer d'un service. L'individu devrait dès lors avoir la possibilité juridique de mettre un terme à cette relation commerciale mais cette possibilité se heurte à la pratique, les données étant par nature volatiles et difficilement maîtrisables une fois créées, la pratique de l'automesure permettant par ailleurs de conduire à leur multiplication.

Ainsi, « les médias numériques posent […] un certain nombre de questions quant à la protection des données personnelles et à la mise en œuvre d'intelligence de la vie privée eu égard aux conditions renouvelées de production/réception d'information et du déploiement d'activité de communication qui leur sont liées »[528]. Cette intelligence de la vie privée se heurte dès lors à la multiplication des services qui sont proposés qui empêche les individus de donner aux traitements de données réalisés un consentement qui soit véritablement univoque, conformément à la définition du consentement donné par l'article 4, 11° du RGPD. Bien qu'un acte positif clair soit requis pour l'obtention du consentement, la multiplication des services nécessitant le consentement et des informations qui y sont relatives empêchent les individus de procéder à leur lecture et font que ceux-ci acceptent des engagements de confidentialité sans en avoir pris vraiment connaissance. Ce phénomène, amplifié par la complexité des termes utilisés par ces engagements, est exacerbé par la valeur marchande que les données représentent pour les entreprises.

---

[526] G29, *Lignes directrices sur le consentement*, op. cit., p. 11.
[527] Stéphanie Hennette-Vauchez, Diane Roman, *Droits de l'Homme et libertés fondamentales*, HyperCours, Dalloz, 3ème édition, juin 2017, p. 577.
[528] Fabien Granjon, « « Du (dé)contrôle de l'exposition de soi sur les sites de réseaux sociaux », *Les Cahiers du numérique*, 2014, Vol. 10, pp. 19-44.

B. La valeur marchande de la donnée

272. Les données personnelles des individus représentent pour beaucoup d'entreprises la première source de revenus à l'ère de l'économie numérique. L'objectif premier d'une collecte aussi intensive de données à caractère personnel par les entreprises est généralement de pouvoir procéder à l'amélioration du service. Mais ces collectes massives « ont également […] de multiples objectifs secondaires »[529] et le puissant potentiel économique des données est renforcé par leur double nature. Celles-ci sont pour les individus des biens immatériels, inaliénables et insaisissables protégés par des droits de la personnalité. Mais elles sont des biens à valeur patrimoniale pour les entreprises du numérique qui vont chercher à les monétiser après avoir recueilli le consentement des individus. Cette exploitation économique des données personnelles, renforcée par leur nature ambivalente, est rendue possible par le développement de la publicité ciblée **(1)** et nécessite d'analyser les risques liés à la commercialisation de telles données **(2)**.

1. Le développement de la publicité ciblée

273. Un *marketing* fondé sur la connaissance de l'individu. A l'heure des b*ig data* et de la collecte massive d'informations, les données à caractère personnel représentent une source importante de revenus pour les entreprises. En effet, celles-ci font reposer la gratuité de leurs services sur la fourniture de données à caractère personnel par l'individu et les éventuelles réutilisations ultérieures permettent le développement exponentiel de la publicité ciblée. De nombreuses techniques de marketing reposent désormais « sur l'enregistrement et le traitement de données personnelles des consommateurs, permettant d'établir des profils de plus en plus précis »[530]. Il devient ainsi vital pour les entreprises du numérique d'avoir accès à de plus en plus d'informations précises sur les individus car l'efficacité des dispositifs publicitaires qui sont mis en œuvre dépend en effet de cette masse d'informations et de la précision dont elles relèvent. Cette logique de *marketing* reposant sur la

[529] Juliette Sénéchal, « La diversité des services fournis par les plates-formes en ligne et la spécificité de leur rémunération, un double défi pour le droit des contrats », *AJCA*, 2016, p.141.
[530] Mathieu Fontaine, Sylvain Juillet, Didier Froger, « La donnée numérique : l'or noir du XXIème siècle ? », *Les Petites Affiches*, 8 septembre 2017, n°179-180, p. 90.

connaissance des individus a trouvé sa source dans le développement des sites commerciaux mais elle a progressivement changé de support pour s'établir sur les réseaux sociaux, les moteurs de recherche, et également sur les applications telles que celles utilisées pour l'automesure.

274. Le recours aux cookies. Le profilage réalisé à des fins publicitaires a pu d'abord être réalisé grâce aux métadonnées qui ont joué un rôle central dans le développement du *marketing* ciblé. Mais les cookies déposés sur les dispositifs des utilisateurs ont permis la pérennisation de ce modèle. Selon la définition de la CNIL, les cookies sont des « traceurs déposés et lus par exemple lors de la consultation d'un site internet, de la lecture d'un courrier électronique, de l'installation ou de l'utilisation d'un logiciel ou d'une application mobile et ce, quel que soit le type de terminal utilisés tels qu'un ordinateur, un *smartphone*, une liseuse numérique et une console de jeux-vidéos connectée à Internet »[531]. Le recueil du consentement, exigé pour avoir recours à l'utilisation de traceurs, n'a cependant pas permis d'éviter certaines dérives, en dépit des premières recommandations fournies par la CNIL[532].

L'adoption de la directive 2009/136/CE, modifiant l'article 5.3 de la directive 2002/58/CE[533], avait permis de préciser l'encadrement du recours aux *cookies* par les entreprises du numérique. Pourtant, dans une décision de mise en demeure du 26 janvier 2016 à l'égard du réseau social Facebook[534], la CNIL a mis en lumière les manquements de cette société quant à l'obligation d'obtenir l'accord préalable des personnes concernées avant d'inscrire des informations sur leur équipement terminal de communications électroniques ou d'accéder à celles-ci. Constatant également qu'un croisement de données à caractère personnel était réalisé à des fins de publicité ciblée, la CNIL a de manière plus générale pointé le défaut d'information délivré aux personnes concernées et les modalités erronées de recueil du consentement, ces éléments s'opposant à ce que la volonté de l'individu soit considérée comme suffisamment éclairée.

---

[531] https://www.cnil.fr/fr/cookies-traceurs-que-dit-la-loi
[532] CNIL, Délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978.
[533] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).
[534] CNIL, Délibération n°2016-007 du 26 janvier 2016 mettant en demeure les sociétés X et Y.

L'article 82 de la loi Informatique et Libertés reprend le dispositif en vigueur qui repose à l'heure actuelle sur la nécessité d'informer « de manière claire et complète » l'individu quant à « la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ». Ces dispositions ont eu pour effet de limiter à 13 mois la durée de vie maximale d'un cookie et des précisions supplémentaires ont été récemment apportées par la CNIL dans le cadre de son plan d'action pour l'année 2019-2020, qui concerne principalement le ciblage publicitaire[535].

275. Des précisions complémentaires. De nouvelles lignes directrices ont ainsi été adoptées en juillet 2019 ; elles auront vocation à être complétées, début 2020, par de nouvelles recommandations. Celles-ci concernent tout particulièrement le consentement qui est donné par l'individu lorsqu'un dépôt de cookies ou autres traceurs est effectué sur le terminal d'un utilisateur. La notion de terminal est entendue largement et de nombreux dispositifs utilisés pour la pratique de l'automesure sont concernés, qu'il s'agisse d'une tablette ou d'un mobile multifonctions (« smartphone »), d'un ordinateur fixe ou mobile, ainsi que « tout autre objet connecté à un réseau de télécommunication ouvert au public »[536]. L'article 2 de la délibération du 4 juillet 2019 a pour objet de préciser les modalités de recueil du consentement lorsque des traceurs sont utilisés sur un terminal, celui-ci devant, conformément aux dispositions du RGPD, reposer sur une manifestation de volonté libre, spécifique, éclairée et univoque de la part de l'utilisateur.

276. Aux Etats-Unis, la Federal Trade Commission (FTC) proposait dès 2007 certains principes et lignes directrices relatifs à la « diffusion de publicité et autres communications personnalisées à destination des internautes »[537]. Une initiative similaire avait été prise en France par la Commission des clauses abusives qui avait fait paraître une recommandation relative aux contrats proposés par les fournisseurs

[535] https://www.cnil.fr/fr/ciblage-publicitaire-en-ligne-quel-plan-daction-de-la-cnil
[536] CNIL, Délibération n° 2019-093 du 4 juillet 2019 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 ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs) (rectificatif).
[537] Françoise Gilbert, « La FTC américaine propose des principes pour encadrer la publicité comportementale sur Internet », *La Gazette du Palais*, 24 avril 2008, n° 115, p. 17.

de réseaux sociaux[538]. Cette recommandation identifiait déjà les risques qu'une information parcellaire, notamment en matière de publicité ciblée[539], pouvait faire courir aux individus.

277. Une concentration de services. Renouvelés aujourd'hui par la pratique de l'automesure, ces risques deviennent le fait d'une concentration des opérateurs appelés à collecter des données. De nombreuses sociétés spécialisées dans l'équipement sportif ont en effet fait l'acquisition d'applications relatives à l'activité physique ou ont développé leur propre application[540]. Procéder ainsi leur permet de recueillir des informations directement auprès des usagers afin de leur proposer des publicités ciblées. Outre cette concentration des données aux fins de ciblage publicitaire, il existe un risque de décontextualisation de celles-ci dès lors qu'elles font l'objet d'une commercialisation.

2. Analyse des risques liés à la commercialisation

278. Le développement d'une économie de la donnée à caractère personnel fondée sur la valorisation par différents services est rendu possible par les caractéristiques même d'une donnée. Non périssable, celle-ci peut par définition être reproduite à l'infini et peut également faire l'objet d'un nombre illimité de transferts successifs sur différents supports et entre les mains de différents prestataires. Les acteurs du numérique, par leur capacité à s'établir en tant que plateformes recueillant un nombre toujours plus important de données, deviennent dès lors dépositaires de pans entiers de la vie personnelle, ce qui les incite notamment à « étendre leur collecte par la diversification des services proposés ou le rachat d'autres acteurs »[541].

[538] Commission des clauses abusives, recommandation n° 2014-02 du 7 novembre 2014 relative aux contrats proposés par les fournisseurs de réseaux sociaux.
[539] Anne Debet, « La Commission des clauses abusives et la protection des données personnelles sur les réseaux sociaux : une incursion hésitante dans un territoire inconnu », *Revue des contrats*, septembre 2015, n°3, p. 496.
[540] Voir par exemple l'application *Map My Fitness* de l'équipementier américain *Under Armour* dont les conditions générales d'utilisation précisent que pour avoir un accès complet au service proposé, l'utilisateur doit renseigner certaines données à caractère personnel. Parmi les modalités d'utilisation de ces données personnelles, l'équipementier indique que celles-ci peuvent servir à contacter directement les individus pour leur proposer des services (« establishing contact with Users to deliver special offers, promotions or other information »), ou améliorer leur activité publicitaire (« Improving our marketing and promotion efforts »).
[541] Laurent Cytermann, *op. cit*, p. 99.

L'objectif pour les entreprises est de pouvoir répondre à un nombre toujours plus important de demandes en services numériques. Restreindre le nombre d'interlocuteurs leur est donc profitable puisqu'elles sont amenées à étendre leur expertise à différents secteurs (réseau social, moteurs de recherche, domotique, santé, cartographie) dans le but d'avoir une connaissance plus précise des individus utilisant de tels services[542]. Le marché de la publicité comportementale en ligne a par ailleurs donné naissance à de nouveaux acteurs, dénommés *data-brokers*, spécialisés dans l'agrégation et la revente de données à caractère personnel à des fins de *marketing* et de ciblage publicitaire[543]. Cette agrégation de données par des tiers au profit d'une publicité toujours plus personnalisée[544] soulève pourtant le risque d'une décontextualisation des informations collectées.

279. Des données décontextualisées. Les données, détachées de tout cadre et du contexte dans lesquelles elles ont été collectées, ne seraient plus forcément révélatrices de traits propres à l'identité de l'individu. Dégagée à partir de l'observation des réseaux sociaux[545], cette hypothèse serait susceptible de s'appliquer aux données agrégées par des régies publicitaires, en l'absence de tout lien concret avec l'individu. Cette rupture du lien avec l'individu est susceptible d'avoir une double conséquence. Celle-ci peut éventuellement empêcher l'identification de l'individu une fois les données transmises à des tiers et décontextualisées. Mais cette décontextualisation empêche également toute possibilité de maîtrise, par l'individu, des données le concernant et ayant fait l'objet de transferts successifs entre différents acteurs.

Les modes de collecte et d'exploitation des données, renforcés par la portabilité croissante de l'informatique, le sont dès lors aussi par des objets connectés dans le cadre d'un *pervasive computing* désignant l'omniscience des outils informatiques utilisés. Les outils employés pour la pratique de l'automesure

[542] Pour une illustration du regroupement de différents services dans le domaine de la fiction, voir notamment Dave Eggers, *The Circle*, Knopf, October 2013.
[543] Pour un exemple concernant spécifiquement le cas de la publicité dans le domaine touristique, voir notamment : Anne-Lise Multin, « Internet - La vente des produits touristiques sur le net, régie par un régime protecteur à l'égard de tous », *Tourisme et Droit*, 2005, n°71, p. 24.
[544] Matthew Crain, « The limits of transparency : Data brokers and commodification », *New Media & Society*, Vol 20, Issue 1, July 2016, pp. 88 – 104.
[545] Serge Gutwirth, Yves Poullet, Paul De Hert, *Data Protection in a Profiled World*, Springer, 2010, p. 124.

connectée, en participant à cette décontextualisation par le recours à différents prestataires, empêcherait également toute tentative de maîtrise, par les individus, des données qu'ils ont contribué à créer.

280. Le risque pour la réputation des individus. Dès 2013, la CNIL confirmait le lien entre la perte de maîtrise des données collectées et les préoccupations relatives à la réputation et à l'image des individus, 34% des plaintes déposées s'y référant. En dehors des dispositions pénales protégeant en théorie les individus des risques relatifs à leur réputation, leur permettre concrètement une meilleure maîtrise de la diffusion de leurs données est apparu indispensable[546]. L'arrêt de la CJUE du 13 mai 2014, instaurant un droit au déréférencement plus communément appelé droit à l'oubli numérique, a illustré ces préoccupations juridiques actuelles en matière de protection de la réputation et des libertés[547]. Renouvelé par la loi pour une République numérique, ce cadre juridique est cependant resté porteur de doutes quant aux capacités effectives de maîtrise de la réputation en ligne[548]. Le droit à l'oubli, désormais consacré à l'article 17 du RGPD[549], servirait au mieux de correctif *ex post* permettant de limiter ce risque dans le temps. Surtout, celui-ci permettrait de tempérer les effets de traitements reposant sur un éventuel consentement faussé de l'individu.

§2. Un consentement faussé

281. Le consentement des individus représente, selon notre système de protection actuelle des données, le préalable nécessaire à la mise en œuvre de tout traitement. En effet, cette opération est en principe libre mais le consentement permet de légitimer le traitement et de s'assurer que les droits dont disposent les individus ont été portés à leur connaissance en amont de la collecte. Le consentement doit permettre une meilleure maîtrise concrète de ses données par l'individu, tout en lui permettant d'exercer un certain nombre de droits : droit d'accès, droit à rectification,

---

[546] CNIL, *Rapport d'activité 2013*, La Documentation Française, 2014, p. 17.
[547] Julien Mucchielli, « L'e-réputation : préoccupation croissante des Français, pour la CNIL », *Dalloz Actualité*, 20 mai 2014.
[548] Jacques Francillon, « De quelques atteintes à la réputation des personnes : e-réputation, cyber-harcèlement, usurpation d'identité numérique, menace de révélation diffamatoire... », *RSC*, 2016, p. 544.
[549] Cf., *infra*, n° 324.

droit à l'effacement ou droit à la portabilité. Pourtant, à l'ère de la généralisation massive des services numériques, le consentement apparaît souvent comme faussé ou reposant tout du moins sur une information obscure et difficilement accessible[550]. Ces éléments, avérés en pratique, ont par exemple justifié la sanction infligée par la CNIL à la société Google en janvier 2019[551].

Les utilisateurs de services d'automesure connectée n'ont pas toujours conscience des modalités selon lesquelles les informations qu'ils divulguent sont utilisées ou réutilisées. Plusieurs facteurs déjà envisagés permettent de contribuer à ce manque d'information. Les promesses liées à l'utilisation de services novateurs sont souvent suivies d'un défaut de lecture des conditions générales d'utilisation relatives à la confidentialité. Ces dernières sont d'ailleurs souvent techniques et complexes et permettent de pérenniser le paradoxe de la vie privée. La contractualisation récente du droit à la protection des données **(A)**, qui contribue à fausser le consentement, permet aux entreprises du numérique de réaliser des opérations dont les personnes concernées n'ont pas conscience et qui pourraient par conséquence échapper à leur contrôle **(B)**.

A. La contractualisation du droit des données personnelles

282. Le G29, dans ses lignes directrices sur le consentement au sens du règlement 2016/679, précise que le traitement de données pour lequel le consentement est sollicité ne peut devenir la contre-performance d'un contrat et que ces deux bases juridiques du traitement, consentement et contrat, ne peuvent être fusionnées et amalgamées. Les données personnelles, envisagées comme étant hors du champ patrimonial en raison de leur nature et de la protection qui leur est apportée, sont pourtant placées au cœur de contrats de prestations de service. Conclus entre le responsable de traitement et la personne concernée, ceux-ci remettent en cause la question du prix par l'échange d'un service théoriquement gratuit contre des données à caractère personnel.

[550] 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 X.
[551] Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC.

Le premier facteur de complexité relatif à ces transactions repose en pratique sur l'identification matérielle de tels contrats. Dans le cas des objets connectés, la vente du dispositif repose sur un contrat de vente classique. Mais les applications qui y sont liées, disponibles *via* des plateformes en ligne et souvent gratuites, ne donnent que peu d'indications sur les termes de l'accord conclu, si ce n'est dans leurs conditions générales d'utilisation. Or, la valeur contractuelle de ces termes **(1)** est susceptible de représenter un risque supplémentaire pour l'individu, au regard de l'absence de négociations portant sur de tels engagements **(2)**.

1. La valeur contractuelle des conditions générales d'utilisation

283. Les rapports entre responsables de traitement et personnes concernées sont fondés sur la délivrance d'un service en échange de données à caractère personnel. Cet accord pose la question du lien juridique existant véritablement entre ces deux parties, notamment à l'égard du droit de la consommation et du commerce électronique, envisagé aussi bien au niveau européen que national[552]. A ce titre, la proposition de directive du Parlement européen et du Conseil du 9 décembre 2015, relatives aux contrats de fourniture de contenu numérique[553], précise dans son article 3.1 son champ d'application. Cette proposition s'applique « à tout contrat par lequel un fournisseur fournit un contenu numérique au consommateur ou s'engage à le faire, en échange duquel un prix doit être acquitté ou une contrepartie non pécuniaire, sous la forme de données personnelles ou de toutes autres données, doit être apportée de façon active par le consommateur ».

284. Le bouleversement induit par le numérique. Ces dispositions permettent d'acter, pour certains auteurs, la reconnaissance « de certains bouleversements induits par le numérique : d'une part, celui de l'établissement du paradigme de l'accès – en l'occurrence aux contenus numériques – en lieu et place de celui de la propriété ; d'autre part, celui de la reconnaissance d'un « échange « non monétaire » pouvant prendre place au sein des contrats de fourniture de contenus

[552] Juliette Sénéchal, « Le contrat de fourniture de contenu numérique en droit européen et français : une notion unitaire ou duale ? », *Revue de l'Union européenne*, 2015, p. 442.
[553] Commission Européenne, Proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique, Bruxelles, le 9 décembre 2015, COM (2015), 634 final, 2015/0287 (COD).

numériques, à savoir celui de l'accès à ces contenus contre des données, à caractère personnel ou non »[554]. La proposition de directive explicite ainsi, au sein d'un instrument législatif européen, la reconnaissance d'une économie fondée sur l'échange d'un contenu en contrepartie de données pouvant présenter un caractère personnel.

Le considérant 13 de la proposition rend particulièrement compte de ce changement de paradigme en indiquant que « dans l'économie numérique, les acteurs du marché ont souvent et de plus en plus tendance à considérer les informations concernant les particuliers comme ayant une valeur comparable à celle de l'argent ». Pourtant, le considérant 14 de la proposition de directive serait susceptible de vider le texte de sa substance en raison notamment de la considération portée aux données [555]. En effet, ce considérant fait reposer l'applicabilité du texte « aux contrats en vertu desquels le fournisseur demande des données, comme un nom et une adresse électronique ou des photos, et le consommateur les lui communique de façon active, directement ou indirectement ». Dès lors, la directive n'a pas vocation à s'appliquer lorsque les données à caractère personnel sont recueillies uniquement pour permettre la fourniture du contenu ou du service numérique par le fournisseur.

Cette limitation est de nature à restreindre considérablement la portée du texte. En effet, toutes les données, recueillies de manière passive par le responsable de traitement lorsque la personne utilise le service, sont exclues du cadre de la directive. Or, ces données potentiellement identifiantes font partie des informations servant à définir le profil de l'individu et sur la base desquelles celles-ci peuvent être monétisées, notamment à des fins de publicité ciblée.

285. Les hésitations sur la qualification du contrat. La qualification du contrat semble soulever certaines interrogations[556]. La reconnaissance des données en tant que contrepartie est de nature à permettre d'envisager leur caractère patrimonial mais, l'absence de droit de propriété sur de telles données s'y oppose en principe.

[554] Judith Rochfeld, « Le « contrat de fourniture de contenus numériques » : la reconnaissance de l'économie spécifique « contenus contre données » », *Dalloz IP/IT*, 2017, p. 15.
[555] *Ibid.*
[556] Laurence Usunier, « Du droit commun européen de la vente aux propositions de directives sur les contrats de vente en ligne et de fourniture de contenu numérique : la montagne accouche d'une souris », *RTD Civ.*, 2016, p. 304.

Comme nous l'avons vu, en l'état actuel, le dispositif contractuel liant fournisseur de contenu numérique et consommateur, responsable de traitement et personne concernée, repose sur le recours aux conditions générales d'utilisation. Celles-ci permettent de déterminer les rapports entre les différentes parties mais elles sont également le moyen pour le responsable de traitement de fournir à la personne concernée l'ensemble des informations qu'elle doit lui communiquer. Cette pratique a d'abord été constatée sur les réseaux sociaux ou « l'internaute conclut d'un clic un contrat après avoir fourni des données personnelles », contrat qui « comporte des conditions générales d'utilisation qui régissent les relations entre le média social et l'utilisateur »[557]. Une solution similaire est applicable aux objets connectés et aux applications de *quantified-self* qui sont susceptibles d'être liées aux dispositifs. Dès lors, « l'intégration des conditions générales d'utilisation dans le champ contractuel […] et leur contractualisation par l'inscription au réseau social » semblent difficilement contestables »[558]. L'enjeu pour l'individu est de pouvoir être informé des clauses qui sont susceptibles de lui être appliquées afin de pouvoir donner un consentement détaillé et éclairé. A ce sujet, le Code de la consommation précise, dans son article R. 132-1, 1°, que sont irréfragablement présumées abusives « les clauses ayant pour objet ou pour effet de constater l'adhésion du non-professionnel ou du consommateur à des clauses qui ne figurent pas dans l'écrit qu'il accepte ou qui sont reprises dans un autre document auquel il n'est pas fait expressément référence lors de la conclusion du contrat et dont il n'a pas eu connaissance avant sa conclusion ». La contractualisation des conditions générales d'utilisation ne devrait donc théoriquement pas nuire à la personne concernée par le traitement. Pourtant, il est de pratique constante que celles-ci ne renseignent pas toujours l'individu de toutes les utilisations qui seront faites de ses données actives ou passives, d'autant que ces conditions ont généralement pour effet de conférer une licence d'utilisation des données au fournisseur de service, responsable du traitement opéré.

286. Le défaut d'accessibilité de l'information. La doctrine a déjà eu l'occasion de constater des manquements au droit de la consommation et au droit à la

[557] Grégoire Loiseau, « La valeur contractuelle des conditions générales d'utilisation des réseaux sociaux », *Communication Commerce électronique*, n°7-8, Juillet 2012.
[558] *Ibid.*

protection des données personnelles dans des conditions générales d'utilisation relatives à un jeu de réalité augmenté et nécessitant le recours à des objets connectés. Celles-ci, susceptibles d'être « contradictoires, pour d'autres incertaines, voir même inintelligibles »[559] ne sont donc pas toujours à même de donner aux individus une information claire et complète sur les informations collectées et sur leurs modalités d'utilisation ultérieures. La sanction infligée par la CNIL à la société Google en janvier 2019[560] permet de synthétiser les différentes critiques qui peuvent aujourd'hui être apportées aux conditions générales d'utilisation et engagements de confidentialité des services proposés. Outre leur défaut de clarté, ceux-ci sont généralement composés d'une multitude de documents qui nuisent à leur accessibilité et ne permettent pas de recueillir le consentement éclairé de l'individu.

La loi pour une République numérique a entendu mettre en œuvre une obligation de loyauté à l'égard des plateformes[561]. Mais le caractère restrictif de la définition du « service de communication au public en ligne »[562] donnée par le texte ne semble pas pouvoir s'appliquer directement aux objets connectés et au *quantified-self* car cette définition concerne majoritairement les opérations de mise en relation entre professionnels et consommateurs ou entre consommateurs entre eux. Par ailleurs, l'absence de négociation relative à l'acceptation de ces conditions générales d'utilisation renforce le déséquilibre existant entre opérateurs du numérique et individus.

2. L'absence de négociation des conditions générales d'utilisation

287. L'autonomie de la volonté. Le principe d'autonomie de la volonté confère en théorie sa force au contrat et aux obligations qui en découlent, selon les principes traditionnels du droit des obligations. Pourtant, la pratique de contrats

[559] Jessica Eynard, « Pokémon GO et le droit : quel cadre juridique pour la réalité augmentée ? », *Les Petites Affiches*, 18 août 2017, n°164-165, p. 5.
[560] CNIL, Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC
[561] Lucie Cluzel-Métayer, « La loi pour une République numérique : l'écosystème de la donnée saisi par le droit », *AJDA*, 2017, p. 340.
[562] L'article 49 de la loi pour une République numérique indique qu'est qualifiée d'opérateur de plateforme en ligne toute personne physique ou morale […] proposant un service de communication au public en ligne reposant sur : le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par

« dans lesquels une partie ne fait qu'adhérer à une convention entièrement préparée par l'autre » s'est répandue[563]. La jurisprudence ne censure pas ce type de contrat et ne leur refuse pas force obligatoire au motif qu'ils n'ont pas été librement négociés[564]. En effet, la forme de l'acceptation est en principe libre et « une case à cocher sur le formulaire d'adhésion, par exemple, permettra de formaliser ce consentement »[565]. En théorie, le destinataire d'une offre est toujours libre de la refuser mais la question de l'application de ces contrats aux services numériques pose la question du choix qui est réellement laissé à l'individu. La transformation numérique d'un grand nombre de services laisse en effet la question de la liberté du consentement en suspens.

Le consentement, au sens du RGPD, s'entend d'une manifestation de volonté libre qui implique un choix et un contrôle réel pour les personnes concernées et qui s'oppose en théorie à ce que le consentement soit présenté comme une partie non négociable des conditions générales, sachant que l'acceptation globale de ces conditions ne peut être considérée comme un acte clair visant à donner son consentement[566]. La conditionnalité du consentement permet déjà au responsable de traitement de collecter des données qui ne sont pas nécessaires à la fourniture du service. Or, l'absence de négociation des CGU s'oppose également à la nécessité de détailler le consentement. Différentes finalités peuvent être mentionnées par les responsables de traitement au sein des CGU ou engagements de confidentialité, entre fourniture du service, publicité ciblée ou encore analyse statistique.

288. Un consentement distinct. Le RGPD précise que lorsque le traitement a plusieurs finalités, le consentement devrait être donné pour l'ensemble d'entre elles[567], le consentement étant présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement

---

des tiers ; ou la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service.

[563] Alain Bénabent, *Droit civil. Les obligations*, Montchrestien, Domat droit privé, 11ème édition, aout 2007, p. 21.

[564] Civ. 1ère, 19 janvier 1982, JCP 1984.II.20215.

[565] Tiphaine Bessière, « La collecte de données personnelles : un cadre précis à respecter », *JS*, 2011, n°111, p.22.

[566] G29, *Lignes directrices sur le consentement*, *op. cit.*, p. 6.

[567] Considérant 32, Règlement (UE) 2016/679.

des données[568]. L'acceptation globale des conditions générales ne peut dès lors pas être considérée comme un acte positif clair visant à donner son consentement et la personne concernée devrait ainsi pouvoir consentir séparément à chacune des finalités qui sont exprimées[569]. Cette exigence relative au recueil d'un consentement détaillé et spécifique se heurte pourtant aujourd'hui à la pratique de l'automesure.

289. Les CGU, par leur manque de clarté, ne permettent généralement pas à l'individu de consentir spécifiquement aux différentes finalités qui sont exposées. Mais le fonctionnement même du *quantified-self*, par l'interconnexion de différents dispositifs, est également susceptible de remettre en question ce principe de liberté du consentement. Dans le cas notamment des objets connectés, la question se pose de savoir si un individu bénéficiant du support matériel et devant avoir recours à une application pour exploiter tout le potentiel de l'objet aura véritablement le choix quant à l'acceptation des termes des conditions générales d'utilisation qui lui sont soumises.

290. Une influence sur le choix de l'utilisateur. Le postulat relatif à l'absence de négociation des conditions générales d'utilisation semble être le propre des contrats d'adhésion ou « la partie faible doit inévitablement en passer par les conditions qu'impose la partie forte »[570]. Or, dans les faits, lorsqu'une demande de consentement est liée à l'exécution d'un contrat par le responsable de traitement, une personne concernée ne souhaitant pas autoriser le traitement de ses données risque de voir les services sollicités lui être refusés. La personne concernée par un éventuel traitement pourra préférer se tourner vers une application payante, dotée de conditions générales d'utilisation plus respectueuses des droits des individus. Le G29 indique pourtant que le consentement ne peut pas être considéré comme donné librement si un responsable de traitement avance qu'il existe un choix entre son service, comprenant le consentement à l'utilisation de données à caractère personnel à des fins complémentaires, et un service équivalent proposé par un autre responsable du traitement. Le fait que différentes applications aux fonctionnalités similaires

[568] Considérant 43, Règlement (UE° 2016/679.
[569] *Ibid.*
[570] Alain Bénabent, *op. cit.*, p. 21.

soient disponibles sur le marché ne permet donc pas de caractériser la liberté du consentement.

L'intelligibilité du texte même des conditions d'utilisation est dans certains cas sujet à controverses en raison du manque de clarté de la formulation et du lexique employé. Les individus acceptent souvent ces termes en cochant des cases pour les accepter et ce sans les lire, en vertu du paradoxe de la vie privée et des efforts disproportionnés pour parvenir à la maîtrise de telles dispositions[571]. Ces différents éléments sont susceptibles de limiter les capacités de contrôle des individus sur leurs données à caractère personnel. Ne pouvant avoir pleinement conscience des modalités d'utilisation auxquelles ils consentent, ceux-ci ne sont pas en mesure de contrôler l'utilisation faite de leurs données. Par ailleurs, en méconnaissance du principe de proportionnalité du traitement par rapport à la finalité déterminée, de nombreuses conditions générales d'utilisation englobe des données sans lien apparent avec cette finalité, influençant également les modalités de collecte de ces informations.

B. La collecte disproportionnée de données personnelles

291. Les conditions de collecte des données à caractère personnel, souvent floues en raison des termes utilisés dans les conditions générales d'utilisation, heurtent dans bien des cas le principe de proportionnalité de la collecte réalisée. Les responsables de traitement conditionnent dans certaines hypothèses la fourniture d'un service à la transmission de données qui ne sont pas nécessaires à ce service et ceux-ci cherchent généralement à s'assurer que les traitements qu'ils mettent en œuvre ont un spectre suffisamment large pour recouvrir des informations sans lien évident avec la finalité réelle du traitement. Cette finalité déterminée associée au traitement sert dans certaines hypothèses à définir la nature des données traitées[572]. Mais, garantissant également que la collecte est limitée au strict minimum au regard de son objectif affiché, cette finalité est aussi remise en cause par le développement du *big data* **(1)** qui vient limiter la portée du consentement de la personne en cas de réutilisations ultérieures de ses données **(2)**.

1. Un principe de finalité contraire à la logique du *big data*

292. Rappelons que la notion de *big data*, relativement récente, se réfère à « la collecte et à l'agrégation de grandes masses de données provenant de différentes sources, dans le but d'extraire de nouvelles informations grâce à des analyses statistiques, descriptives ou prévisionnelles »[573]. Traduite en français sous l'appellation de « grands ensembles de données », cette collecte est susceptible, en pratique, de menacer la pérennité des principes fondamentaux de la loi Informatique et Libertés. En effet, « le droit à la protection des données personnelles fondé sur la finalité de la collecte s'oppose à la logique de collecte massive du *big data* », puisque celui-ci « permet à l'individu de limiter l'accès à ses données afin de lui laisser le choix de dévoiler tout ou partie de sa personnalité, alors que le *big data* cherche à accéder à un maximum de données »[574]. Cette volonté de collecte exponentielle de données pour des raisons qui ne sont pas connues à l'avance est susceptible d'empêcher l'individu de disposer d'une plénitude de contrôle sur les informations qui sont révélées.

293. Les *data shadows*. Les données personnelles des individus ont vocation à être collectées et à faire l'objet d'un traitement et celles-ci sont complétées par des données en théorie non identifiantes et relatives à l'usage du service. Or, les « Big Data ne tiennent pas compte uniquement des empreintes numériques laissées par les individus – c'est-à-dire des traces qu'ils ont laissées derrière eux » car en effet, ceux-ci « tiennent compte aussi des *data shadows* – à savoir les informations relatives à certains individus, produites ou divulguées par d'autres individus »[575]. Dès lors, le recours aux objets connectés ou à des applications dans le cadre plus général du *big data* permet de collecter des informations relatives à la personne procédant à son

---

[571] Aleecia M. McDonald, Lorrie Faith Crano, « The cost of reading privacy policies », *I/S : A Journal of Law and Policy for the Information Society*, vol. 4, no. 3, 2008-2009, pp. 543-568.
[572] Cf., *supra*, n° 194.
[573] Danièle Bourcier, Primavera De Filippi, *Open Data & Big Data, Nouveaux défis pour la vie privée*, Mare & Martin, Droit & Sciences Politiques, 2016, p. 23.
[574] Éléonore Scaramozzino, « Les enjeux juridiques du big data », *JT* 2017, n°201, p.35.

[575] Primavera De Filippi, « Gouvernance algorithmique : vie privée et autonomie individuelle à l'ère des Big Data », *in* Danièle Bourcier, Primavera De Filippi (dir.), *op. cit.*, p. 107.

automesure, mais également à des tiers. Les traces laissées par ces derniers peuvent donc être intégrées au champ d'analyse des grands ensembles de données.

Indirectement concernés par les traitements mis en œuvre, les tiers ne sont pas toujours en mesure d'exprimer valablement leur consentement. Ceux-ci, malgré les dispositions de l'article 14 du RGPD, ne sont en effet pas toujours informés que de telles informations sont collectées. L'application de course à pieds *Runtastic* indique par exemple, au point 2.3 de son engagement de confidentialité relatif aux données additionnelles de l'utilisateur (dans sa version du 13 novembre 2017) que celles relatives à ses liens d'amitié (« *friendships* » dans le texte) peuvent être collectées, sans pour autant en préciser la portée exacte ni la finalité, bien que l'on puisse en déduire qu'il s'agit d'autres utilisateurs de l'application connectés au réseau de l'individu. Les capacités de partage des informations relevées dans le cadre du *quantified-self* sur des réseaux sociaux renforcent ce constat en ce que les modalités d'interaction entre le réseau et l'application sont susceptibles de fournir à celle-ci la liste des contacts de l'individu.

294. La corrélation d'informations. Par ailleurs, les capacités d'interconnexion des objets connectés, applications ou *smartphones*, font que les responsables de traitement peuvent affiner l'analyse proposée également grâce à des données collectées auprès de tiers ou d'autres objets[576]. De telles opportunités s'inscrivent pleinement dans la logique relative au *big data* et permettent une interconnexion plus étendue de données, susceptible de produire également de plus en plus de résultats relatifs à l'analyse. Les conditions générales d'utilisation et engagements de confidentialité des différents services prévoient dans certains cas explicitement cette fonction d'analyse en tant que finalité du traitement initial. Mais la portée des différentes interconnexions réalisées n'est pas toujours maîtrisée par l'utilisateur, affaiblissant non seulement le consentement qu'il donne en amont du traitement, mais également celui qu'il est censé fournir en cas de réutilisation ultérieure de ses données.

[576] Voir par exemple l'engagement de confidentialité relatif à l'application *My Net Diary* permettant de compter le nombre de calories ingérées et qui précise explicitement que le site, support de l'application, est susceptible de combiner des

2. Un consentement à la portée limitée en cas de réutilisations ultérieures

295. Le système juridique mis en place à partir de 1978 fait du consentement de la personne concernée par un traitement l'élément permettant de légitimer celui-ci. Renouvelé par le RGPD, le consentement préalable reste l'élément central du dispositif et celui-ci repose sur l'information « concise, aisément accessible et facile à comprendre » [577] de l'individu. Censée tempérer le paradoxe relatif à la vie privée et réduire l'étendue du risque informationnel, cette information est pourtant difficilement accessible. Les conditions relatives aux modalités de réutilisation des données sont généralement complexes à déchiffrer pour l'utilisateur et elles ne précisent pas toujours les finalités relatives à de telles réutilisations.

L'intervention de différents opérateurs dans la chaîne de traitement de données, commune dans le cadre du *quantified-self*, rend l'identification des tiers impliqués souvent complexe et ne permet pas toujours de savoir quelle utilisation est faite des données recueillies. De nombreuses applications expriment dans leurs conditions générales d'utilisation ou dans leurs engagements de confidentialité qu'elles n'ont pas de contrôle sur les utilisations qui seraient faites par la suite par d'éventuels sous-traitants ou tiers à qui ils sont susceptibles de transmettre des données[578]. Une telle situation a donc pour effet de représenter une charge supplémentaire pour l'individu. Celui-ci doit déterminer si des données à caractère personnel le concernant sont transmises à un tiers qu'il doit identifier afin de pouvoir se référer aux conditions générales d'utilisation et vérifier dans chaque cas l'utilisation qui sera faite de ses données personnelles.

296. Par ailleurs, les modalités d'accès des données par des tiers ne sont pas toujours précisées par les engagements de confidentialité des responsables de traitement. Le réseau social *Facebook* aurait par exemple permis l'accès à un grand

---

informations directement collectées avec des informations obtenues auprès de tiers (« MyNetDiary.com may combine information about you that we have with information we obtain from business partners or other companies »).

[577] Considérant 58, Règlement (UE) 2016/679.
[578] Voir par exemple l'engagement de confidentialité relatif à l'application de fitness *Sworkit* qui indique : « As a result, we may provide your personal data to a third party company, because we do not control the privacy practices of these third party companies, you should read and understand their privacy policies ».

nombre de données personnelles via un sous-traitant, par le biais d'un système permettant à des applications tierces d'accéder non seulement aux données des usagers ayant utilisé l'application mais aussi à celles de leurs amis[579]. Cette solution peut être transposée au cas de l'automesure connectée : les capacités de partage des données créées par l'utilisation de services de *quantified-self* sur les réseaux sociaux rendent ces données susceptibles d'être concernées par de telles transmissions à des tiers et pour lesquels l'individu n'a pas donné son consentement.

297. La difficulté d'accès à l'information. La chaîne de transmission des données de l'utilisateur est susceptible d'être reproduite indéfiniment. Les tiers peuvent eux-mêmes transmettre les données à d'autres opérateurs soumis à des conditions générales d'utilisation à nouveau différentes. La personne concernée par le traitement doit ainsi procéder à la lecture d'un nombre considérable d'éléments si elle souhaite pouvoir réellement maîtriser l'utilisation qui est réalisée de ses données[580]. La délibération de la CNIL n°SAN-2019-001 du 21 janvier 2019 prononçant une sanction à l'encontre de la société Google LLC relève par exemple que « les informations qui doivent être communiquées aux personnes en application de l'article 13 sont excessivement éparpillées dans plusieurs documents : Règles de confidentialité et conditions d'utilisation , affiché au cours de la création du compte, puis Conditions d'utilisation et Règles de confidentialité qui sont accessibles dans un deuxième temps au moyen de liens cliquables figurant sur le premier document. Ces différents documents comportent des boutons et liens qu'il est nécessaire d'activer pour prendre connaissance d'informations complémentaires. Un tel choix ergonomique entraine une fragmentation des informations obligeant ainsi l'utilisateur à multiplier les clics nécessaires pour accéder aux différents documents. Celui-ci doit ensuite consulter attentivement une grande quantité d'informations avant de pouvoir identifier le ou les paragraphes pertinents. Le travail fourni par l'utilisateur ne s'arrête toutefois pas là puisqu'il devra encore recouper et comparer les informations

[579] Anaïs Moutot, « Affaire Cambridge Analytica : Zuckerberg reconnaît des « erreurs » », Les Echos, 21 mars 2018, accessible en ligne : https://www.lesechos.fr/tech-medias/hightech/0301468858898-facebook-contre-attaque-dans-laffaire-cambridge-analytica-2163127.php

collectées afin de comprendre quelles données sont collectées en fonction des différents paramétrages qu'il aura pu choisir ».

Faire reposer sur l'individu le soin de déterminer les tiers concernés et les utilisations ultérieures des données ne fait en théorie que renforcer le paradoxe relatif à la vie privée puisque ces pratiques sont susceptibles de décourager l'individu face à toute tentative de maîtrise de ses données personnelles. Ces différents éléments, de nature à fausser le consentement qui est donné à l'origine et en amont du traitement, sont également révélateurs des limites des principes protecteurs de la réglementation.

298. Conclusion du chapitre. La conception européenne de la protection des données à caractère personnel s'oppose aujourd'hui à l'idée d'un droit de propriété conféré aux individus sur leurs données. Une solution inverse a en effet été retenue, fondée sur la reconnaissance d'un droit de la personnalité : des droits ont été conférés à l'individu sur ses données afin de rendre possible la mise en œuvre concrète du droit à l'autodétermination informationnelle. L'exercice concret de ce droit se heurte pourtant aujourd'hui à des services qui se nourrissent, pour leur fonctionnement, de données à caractère personnel. Les sites de commerce en ligne ou les réseaux sociaux avaient déjà recours à ce mode de fonctionnement. Mais l'automesure connectée vient généraliser ces procédés : les dispositifs utilisés ont besoin, pour fonctionner, d'être constamment alimentés en données. La nécessité d'obtenir le consentement libre et éclairé de l'individu fait partie des fondements légaux permettant de procéder à un traitement de données. Mais la portée de ce consentement est aujourd'hui remise en question, contribuant à entretenir le risque informationnel qui pèse sur les individus.

CHAPITRE II – L'INSUFFISANCE DES PRINCIPES PROTECTEURS

299. Les données récoltées dans le cadre de la pratique de l'automesure sont, malgré de larges difficultés d'appréciation, identifiées par la réglementation comme étant des données personnelles ou des données personnelles sensibles. L'individu concerné par ces données doit alors bénéficier des dispositions protectrices qui relèvent d'une telle qualification. Le régime juridique en place a vocation à s'appliquer lorsqu'une donnée à caractère personnel fait l'objet d'un traitement, défini comme tout « ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé »[581].

300. Protecteur dans son principe, le régime juridique ne se veut pas pour autant trop restrictif dans son application pratique[582]. En effet, le droit à la protection des données tend simplement à « établir les règles du jeu, à établir des équilibres entre des aspirations et des intérêts différents, concurrent parfois contradictoires dans une société ouverte et démocratique »[583]. La réglementation, en instaurant un régime juridique protecteur, n'a pas voulu interdire les traitements de données à caractère personnel. Un compromis a donc été instauré entre le besoin d'assurer d'une part « que des données à caractère personnel puissent circuler librement d'un Etat à l'autre », tout en veillant d'autre part à ce que « les droits fondamentaux des personnes soient sauvegardés »[584].

Le régime de protection *ex ante* mis en œuvre avant l'entrée en application du RGPD reflétait déjà cette liberté de traitement et la réglementation publique venait seulement définir les règles de protection auxquelles les exploitants de données

[581] Article 2, loi Informatique et Libertés telle que modifiée par la loi du 6 août 2004.
[582] Laurent Cytermann, « La loi Informatique et Libertés est-elle dépassée ? », *RFDA*, 2015, p. 99.
[583] Emilie Debaets, *Le droit à la protection des données personnelles, Recherche sur un droit fondamental*, Thèse pour obtenir le grade de docteur de l'Université Paris 1 Panthéon-Sorbonne, présentée et soutenue publiquement le 12 décembre 2014, p. 12.
[584] Considérant n° 3, Directive 95/46/CE.

devaient se conformer[585]. Cette liberté de traitement des données a justement permis le développement du web relationnel, paradigme nouveau selon lequel la divulgation de données personnelles est la condition nécessaire à l'existence du service lui-même[586]. Les individus sont ainsi devenus des « acteurs de premier plan de la production, de la diffusion et de la consommation de données et d'informations »[587]. La Convention 108 du Conseil de l'Europe a été le premier texte à incorporer ce besoin de compromis entre liberté de circulation de l'information et protection des données personnelles[588]. La directive 95/46/CE a par la suite consacré cette libre circulation des données personnelles tout en rappelant la nécessité de protéger « les libertés et droits fondamentaux des personnes physiques »[589].

Ce régime juridique a permis la mise en œuvre par les Etats d'une protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard de tels traitements[590]. Renouvelés par le RGPD, les principes protecteurs mis en oeuvre par la réglementation sont aujourd'hui remis en question par le déploiement à grande échelle d'objets connectés aux capacités de collecte et d'analyse démultipliées. A l'origine du développement de nouveaux services informatiques, cette liberté encadrée de mise en œuvre de traitements de données **(section 1)** semble aujourd'hui difficilement maîtrisable par les principes protecteurs contenus au sein de la réglementation **(section 2)**.

---

[585] Alain Rallet, Fabrice Rochelandet, « La régulation des données personnelles face au web relationnel : une voie sans issue ? », *Réseaux*, n°3, 2011, p. 17 à 47.
[586] Sara M. Watson, *Living with Data : Personal Data Uses of the Quantified-Self*, Oxford Internet Institute Masters Thesis, 2013, p. 34.
[587] Bénédicte Rey, « Les intelligences numériques des informations personnelles. Vers un changement de perspective pour garantir le droit à la vie privée ? », *Les Cahiers du numérique*, 2014/1, Vol. 10, pp. 9-18.
[588] Le préambule de la Convention 108 du Conseil de l'Europe mentionne expressément « l'intensification de la circulation à travers les frontières des données à caractère personnel faisant l'objet de traitements automatisés » tout en réaffirmant l'engagement des Etats membres du Conseil de l'Europe « en faveur de la liberté d'information sans considération de frontières ».
[589] Le considérant 3 du Règlement (UE) 2016/679 reprend cette idée et fait ainsi directement référence à la directive 95/46/CE en indiquant que celle-ci « vise à harmoniser la protection des libertés et droits fondamentaux des personnes physiques ».
[590] Francesco Maiani, « Le cadre réglementaire des traitements de données personnelles effectués au sein de l'Union européenne », *RTD eur.*, 2002, p. 283.

SECTION I. LA LIBERTÉ DE PRINCIPE DU TRAITEMENT

301. Le *quantified-self,* en permettant la collecte de données personnelles, au titre desquelles figurent les données sensibles, vient naturellement mobiliser l'arsenal juridique relatif à la protection de ces informations. Libre dans son principe, la collecte et le traitement de telles données engagent donc la mise en œuvre d'un ensemble de règles permettant d'assurer la protection de l'individu. Ces règles, qui président à la mise en œuvre d'un traitement, on vocation à régir non seulement la façon dont ces données sont collectées, mais également les droits qui sont conférés à l'individu. Une obligation positive d'organiser un contrôle de l'utilisation des données personnelles est dès lors conciliée avec l'impossibilité d'échapper à des traitements de données « dans la vie sociale telle qu'elle est aujourd'hui organisée »[591].

Des principes protecteurs, censés conférer à l'individu des droits lui permettant d'agir sur les traitements dont il fait l'objet, sont mis en place par la réglementation. A l'origine limités, ces droits ont progressivement été renforcés, allant de pair avec l'instauration d'un principe de libre circulation des données personnelles. D'abord consacrée par la directive 95/46/CE[592], cette volonté de libéralisation des échanges de données est réitérée par le RGPD, au nom du développement de l'économie numérique dans l'ensemble du marché intérieur[593]. En renouvelant le cadre juridique applicable aux traitements de données, le Règlement procède à une révolution copernicienne des modalités de protection des traitements[594]. Pourtant, celle-ci reste fondée sur des principes protecteurs déjà applicables et aujourd'hui mis à l'épreuve par l'automesure connectée. Visant à garantir une capacité d'action aux individus faisant l'objet de traitements **(Paragraphe 1)**, ceux-ci ne permettent en réalité qu'une maîtrise limitée des opérations de collecte **(Paragraphe 2)**.

---

[591] Guillaume Desgens-Pasanau, « Informatique et libertés, une équation à plusieurs inconnues », *in* Girot Jean-Luc (dir.), *Le harcèlement numérique*, Dalloz, 2005, p. 97.
[592] Le considérant 3 du Règlement (UE) 2016/679 indique précisément que « la directive 95/46/CE du Parlement européen et du Conseil vise […] à assurer le libre flux des données à caractère personnel entre les Etats membres.
[593] Considérant 7, Règlement (UE) 2016/679.
[594] Cf., *infra*, n° 590.

§1. Une capacité d'action limitée

302. Pour être conforme à la réglementation Informatique et Libertés, un traitement de données doit être réalisé et poursuivi en conformité avec un certain nombre d'obligations. Principalement mises à la charge du responsable de traitement, celles-ci s'accompagnent de droits que l'individu doit être mis en mesure d'exercer. Ce régime juridique n'a pas été mis en œuvre en prenant en considération le développement spécifique de l'automesure connectée. Celle-ci, par ses caractéristiques, vient remettre en question l'application pratique des droits garantis aux individus. Son caractère ubiquitaire limite en pratique la transparence qui doit être associée aux traitements **(A)** et vient restreindre le spectre des droits garantis aux individus **(B)**.

A. La transparence limitée du traitement

303. Le principe de transparence à l'œuvre, explicité entre autres par le considérant 58 du RGPD, vise notamment les cas où il est « difficile pour la personne concernée de savoir et de comprendre si des données à caractère personnel la concernant sont collectées, par qui et à quelle fin ». Ce principe doit donc permettre à la personne, conformément à la position déjà adoptée par le contrôleur européen de la protection des données, de savoir et de comprendre si des données à caractère personnel la concernant sont collectés[595]. Non seulement l'information doit être délivrée, mais celle-ci doit également l'être « d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples »[596]. Un individu téléchargeant une application de *quantified-self* ou utilisant un dispositif connecté doit donc avoir été mis en mesure d'avoir accès à ces informations, préalablement à l'utilisation de ces services. De telles précisions, remises en question par la pratique de l'automesure[597], sont révélatrices d'une prise en compte limitée de l'innovation par la réglementation **(1)** ainsi que du rôle central qui est conféré à l'information de la personne **(2)**.

---

[595] Contrôleur européen de la protection des données, « Relever les défis des données massives : Un appel à la transparence, au contrôle par l'utilisateur, à la protection des données dès la conception et à la reddition de comptes », Avis n°7/2015, p. 5.
[596] Article 12, Règlement (UE) 2016/679.
[597] Cf., *supra*, n° 286.

1. La prise en compte limitée du développement de l'innovation

304. Les nouvelles technologies utilisées dans le cadre du *quantified-self* questionnent la pertinence du cadre juridique relatif aux données personnelles. En effet, le développement croissant des outils numériques de collecte utilisés remet en cause l'efficacité des règles protectrices des droits et libertés des individus. La question de l'adéquation du cadre juridique aux évolutions technologiques est posée et le législateur, national ou européen doit ainsi trouver un juste équilibre : adopter une réglementation protectrice des données à caractère personnel tout en évitant que celle-ci soit susceptible d'empêcher le développement de l'innovation. De telles considérations sont essentielles en matière d'automesure connectée. Sans la recherche d'un tel équilibre, les objets techniques utilisés dans le cadre de l'automesure ne pourraient être développés et à l'inverse, une réglementation trop laxiste pourrait nuire aux droits des individus. La mise en œuvre d'un principe de précaution, jugé trop restrictif, a laissé sa place aujourd'hui à la mise en œuvre d'une liberté d'innovation maîtrisée.

a. Un principe de précaution restrictif

305. Les réseaux sociaux et le web-relationnel montrent que le cœur du sujet communicationnel est aujourd'hui confronté à un changement profond, notamment par la modification du comportement des utilisateurs qui, « de simples lecteurs contemplatifs, sont devenus acteurs-contributeurs »[598]. Cette transition est favorisée par l'échange renouvelé et constant de données permis par les objets connectés dans le cadre de l'automesure connectée. Or, qu'il s'agisse de l'ancienne loi Informatique et Libertés de 1978 ou de la Convention 108 du Conseil de l'Europe en date de 1981, fondements du cadre juridique actuel, cet échange renouvelé de données personnelles n'a pas été prévu. Surtout, ces textes n'ont pas pu prévoir le développement et la connexion d'objets du quotidien servant à réaliser l'ensemble des mesures que l'on retrouve dans le cadre du *quantified-self*.

[598] Franck Confino, « Le « choc » du numérique sur la gouvernance, les enjeux et les stratégies de communication des collectivités locales », *AJCT*, 2014, p. 595.

306. Le législateur pourrait être tenté, au vu des nombreux développements technologiques, de mettre en œuvre un principe de précaution. Le lien entre ce principe et le développement de l'innovation par les objets connectés a été fait par certains auteurs[599]. En effet, « quoiqu'il provienne du secteur de la protection de l'environnement, le principe de précaution tend à s'appliquer à d'autres domaines au hasard des lois », et ce dernier devrait ainsi être pris et mobilisé avant un fait ou une action susceptible de générer le risque d'un préjudice, « lequel serait pris en compte par la responsabilité pour être compensé par une indemnisation »[600]. Cette approche, issue de la Charte de l'environnement et intégrée en 2004 à la Constitution, semble cependant limitative puisqu'elle est susceptible de représenter un frein pour l'innovation.

Le principe de précaution[601], tel qu'il est défini par les textes européens et nationaux[602], ne doit donc pas se montrer restrictif et empêcher le développement de certaines innovations, telles que celles qui sont permises par les objets connectés et l'Internet des objets dans le domaine de la santé[603]. Il semble dès lors impératif que les mesures de protection mises en œuvre ne puissent déboucher sur une restriction des capacités d'innovation qui empêcherait, à ce titre, d'exploiter les données collectées dans le cadre du *big data*[604].

b. Une liberté d'innover encadrée

307. La loi du 20 juin 2018, faisant suite à l'adoption du Règlement européen, a permis d'adapter la loi Informatique et Libertés aux nouvelles dispositions européennes. Cependant, malgré une réforme complétée par le Règlement, « la lecture de la loi du 6 janvier 1978 peut avoir pour le citoyen un caractère déroutant, car les termes correspondants à son expérience quotidienne des usages numériques n'y

---

[599] Thierry Piette-Coudol, *Les objets connectés, Sécurité juridique et technique*, Lexis Nexis, Actualité, 2015, p. 25.
[600] *Ibid.*
[601] Voir par exemple : Arnaud Gossement, *Le principe de précaution*, Thèse de doctorat en droit public, Université Paris-I Panthéon-Sorbonne, 2001, 454 p. ; Pierre-Laurent Frier, *Principe de précaution et sécurité sanitaire*, Thèse de doctorat en droit public, Université Paris-I Panthéon-Sorbonne, 2001, 574 p.
[602] Jean-Simon Cayla, « Le principe de précaution, fondement de la sécurité sanitaire », *RDSS*, 1998, p. 491.
[603] Pour plus de précisions, voir notamment : Eric Topol, *The Creative destruction of medicine : How the digital revolution will create better health care*, Basic Books, 2012, 336 p.
[604] Adam Thierer, « The Internet of Things and Wearable Technology : Addressing Privacy and Security Concerns without Derailing Innovation », *Richmond Journal of Law & Technology*, n°6, 2015, 118 p.

figurent pas »[605]. En effet, des notions telles que celles relatives au *big-data*, au *quantified-self*, aux *smartphones* ou encore aux applications ne sont pas expressément mentionnées dans le texte.

308. Pourtant, et comme cela a été relevé dès 2014 par le Conseil d'Etat, ce « paradoxe ne serait qu'apparent »[606]. La généralité des termes adoptés par la loi Informatique et Libertés a permis à celle-ci de faire face aux évolutions technologiques. Ainsi, les différentes notions envisagées dans l'ensemble du corpus de textes relatifs à la protection des données, qu'il s'agisse des notions de donnée à caractère personnel, de traitement, de finalité ou encore de responsable de traitement « se sont avérées suffisamment plastiques pour s'appliquer à des phénomènes aussi divers que la géolocalisation, la biométrie, les cookies »[607]. La problématique relative aux objets connectés et à l'automesure connectée, sans marquer un coup d'arrêt à cette adaptabilité des différents termes utilisés par la réglementation, interroge pourtant la pertinence du régime juridique applicable, qui repose sur l'information de la personne concernée.

2. Le rôle de l'information de la personne concernée

309. Le principe de libre circulation des données à caractère personnel, consacré en premier par la directive 95/46/CE, établit une liberté d'échange et de transmission des informations, y compris identifiantes. Le consentement préalable de l'individu, « procédé original de simplification administrative »[608] est alors apparu comme le moyen de légitimer cette liberté de traitement. Absent de la Convention 108 du Conseil de l'Europe et de la rédaction initiale de la loi Informatique et Libertés de 1978 – exception faite des données sensibles – le consentement s'est vu reconnaître, avec la directive de 1995, le rôle de fondement légitime à la collecte de données personnelles. Devant être « indubitable »[609], ce consentement a, avant

[605] Laurent Cytermann, « La loi Informatique et libertés est-elle dépassée ? », *RFDA*, 2015, p. 99.
[606] *Ibid*.
[607] *Ibid*.
[608] Nicolas 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.
[609] CJUE, Gr. Ch., 9 novembre 2010, Affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke GbR et Hartmut Eifert contre Land Hessen*, §64 ; *Rtd eur*., 2011. 375, chron. A. Potteau.

l'adoption du RGPD, fait l'objet de différentes interprétations[610] qui ont confirmé son statut de base légale du traitement[611].

310. Une double fonction de l'information. L'obligation d'obtenir le consentement de la personne est renouvelé par le RGPD. Celui-ci donne pour la première fois une définition précise du consentement[612] qui est fourni sur la base de l'information préalable de la personne concernée[613]. Condition de licéité de la mise en œuvre d'un traitement, cette obligation d'information a donc un double rôle :

1). Présentées à l'article 13 du RGPD, les informations fournies au moment du recueil des données doivent permettre à l'individu de connaître l'identité du responsable de traitement, la finalité poursuivie par un tel traitement ou encore les destinataires ou catégories de destinataires des données collectées. L'information délivrée à la personne concernée par le traitement doit donc permettre à celle-ci de donner un consentement éclairé, au sens de l'article 4, 11° et dont les modalités de recueil sont précisées à l'article 7.

2). Outre sa fonction relative au consentement éclairé, le droit à l'information qui est inséré au chapitre III relatif aux droits de la personne concernée, apparaît également comme « la base du dispositif mis en place puisqu'il constitue le préalable nécessaire à l'exercice des autres droits », étant donné qu'il n'est « pas possible de s'opposer à un traitement ou bien d'y avoir accès si l'on n'en connaît pas l'existence »[614]. L'obligation d'information de la personne concernée permet donc à l'individu de pouvoir consentir en toute connaissance de cause à un traitement de données, mais elle apparaît également comme le curseur dont l'étendue lui permettra l'exercice de l'ensemble des droits qui sont conférés par la réglementation.

La délivrance effective de cette information est pourtant remise en question aujourd'hui par la contractualisation des conditions générales d'utilisation des

[610] G29, Avis n° 15/2011 sur la définition du consentement adopté le 13 juillet 2011, WP 187.
[611] CNIL, Délibération n° 2009-474 du 23 juillet 2009 portant recommandation en matière de transfert de données à caractère personnel dans le cadre de procédures judiciaires américaines dite de « Discovery ».
[612] Nathalie Metallinos, « 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.
[613] Article 13 et 14, Règlement (UE) 2016/679.
[614] Marie-Claire Ponthoreau, « La protection des personnes contre les abus de l'informatique », *RFDA*, 1996, p. 796.

services utilisés[615]. Outre des effets sur la portée du consentement qui est donné, l'information parcellaire fournie par les opérateurs de services numériques constitue un frein à l'exercice, par l'individu, de l'ensemble de ses droits. La sanction prononcée en janvier 2019 à l'encontre de la société Google[616] relevait déjà cette difficulté, pour l'individu, à pouvoir exercer la plénitude de ses droits. Le défaut d'accessibilité de l'information, relevé dans cette décision et transposable au domaine de l'automesure en raison de la connexion d'un nombre important de services, vient donc limiter le spectre des droits qui sont en théorie conférés à l'individu.

B. Le spectre limité des droits de l'individu

311. L'interconnexion d'objets et de dispositifs dans le cadre du *quantified-self* ainsi que leur connexion à Internet de manière plus générale, sont révélateurs des nouveaux enjeux attachés à l'expression de son consentement par l'individu[617]. L'information parcellaire sur lequel il repose est pourtant susceptible de remettre en cause le principe de loyauté de la collecte, tel qu'il est notamment exprimé à l'article 5 du RGPD. Les individus se retrouvent donc parfois dans l'impossibilité de s'opposer à la mise en œuvre de traitements **(1)** et d'accéder aux données qui sont collectées à leur égard **(2)**.

1. Le droit d'opposition

312. L'autodétermination informationnelle, telle qu'elle a déjà été présentée, consiste en la faculté de l'individu à pouvoir déterminer avec précision les modalités selon lesquelles des données le concernant sont collectées et utilisées. Mais cette autodétermination informationnelle, bien que limitée, suppose aussi la faculté de pouvoir s'opposer à la mise en œuvre d'un traitement. Ce droit était déjà reconnu par la directive de 1995 qui faisait référence, dans son article 38, aux raisons prépondérantes et légitimes tenant à la situation particulière de l'individu permettant

[615] Cf., *supra*, n° 286.
[616] CNIL, Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC.
[617] Yves Poullet, « La loi des données à caractère personnel : un enjeu fondamental pour nos sociétés et nos démocraties ? », *Legicom*, 2009/1, N° 42, p. 47 à 69.

de s'opposer au traitement. L'article 21 du RGPD indique désormais que « la personne concernée a 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 […], y compris un profilage fondé sur ces dispositions ».

Celui-ci précise également que lorsque les données à caractère personnel sont traitées à des fins de prospection, « la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant à de telles fins de prospection, y compris au profilage ». Le droit d'opposition ne concerne donc pas directement le traitement qui a été réalisé sur le fondement du consentement de l'individu. En effet, dans ce cas, l'individu devra procéder au retrait de son consentement. Ici, le droit d'opposition concerne en premier lieu les traitements qui sont fondés sur l'intérêt légitime du responsable de traitement, apprécié selon le G29, à propos de la directive de 1995, en fonction de la mise en balance avec les intérêts et droits fondamentaux des personnes concernées[618].

313. L'exception fondée sur l'intérêt légitime du responsable de traitement. Le G29 indique à titre d'illustration que les responsables de traitement peuvent avoir un intérêt légitime à connaître les préférences de leurs clients pour être en mesure de mieux personnaliser leurs offres et proposer des produits et services qui correspondent mieux aux besoins et désirs des clients. Dans cette hypothèse, l'intérêt légitime peut servir de fondement à certains types d'activité de prospection et de nombreuses applications le formulent directement. Celles-ci devraient dès lors explicitement mentionner que l'utilisateur dispose du droit de s'opposer à un tel traitement de données, réalisé dans un objectif de prospection commerciale. La portée de cet intérêt légitime semble pourtant difficile à déterminer et peut être porteuse d'un risque de sécurité juridique pour l'individu : celui-ci doit être en mesure de savoir quand il peut valablement s'opposer à un traitement de données. Plusieurs exemples ont été mentionnés par le G29 dans son avis sur la notion d'intérêt légitime, dont certains permettent de mieux en comprendre les enjeux à l'égard de l'automesure.

---

[618] G29, *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, WP 217*, adopté le 9 avril 2014.

Dans un cas, une personne commandant un repas en ligne et ne s'opposant pas à l'envoi d'offres commerciales sur le site du restaurant, reçoit des offres de réduction pour des produits similaires. Ici, l'intérêt du restaurant à envoyer une promotion au client est légitime : le traitement de données réalisé est minime et les droits de la personne concernée ne devrait donc pas justifier la mise en place d'un outil permettant de s'opposer facilement au traitement. Le G29 donne également l'exemple de la vente des données relatives aux habitudes de consommation de l'individu par le restaurant à une compagnie d'assurance qui s'en sert pour ajuster ses primes d'assurance santé. Ici, malgré l'intérêt légitime de la compagnie à évaluer les risques sanitaires auxquels s'exposent ses assurés, l'intérêt et les droits de la personne devraient prévaloir sur ceux de la compagnie, en raison de la collecte excessive qui est réalisée et de la déduction de données sensibles qui est effectuée.

Dans ce cas de figure, l'intérêt légitime du responsable de traitement ne pourra pas être invoqué pour passer outre l'opposition de la personne concernée, des sanctions étant notamment prévues à l'article 226-18-1 du Code pénal. Ce fondement ne pourra donc pas, par exemple, être avancé par le développeur d'une application permettant à l'individu de mesurer le nombre de calories ingérées pendant un repas et qui transmettrait les informations relevées à une compagnie d'assurances. Surtout, outre cette notion d'intérêt légitime qui peut être avancée pour contourner l'opposition de la personne concernée, aucune exception n'est prévue par l'article 21, 3° du RGPD lorsque celle-ci s'oppose au traitement à des fins de prospection. L'individu devra simplement être en mesure de s'opposer au traitement. Or, selon le point 5 de l'article 21, l'exercice de ce droit pourra, dans le cadre de l'utilisation de services de la société de l'information, être réalisable à l'aide de procédés automatisés utilisant des spécifications techniques.

314. L'enjeu pour l'individu en matière de *quantified-self*, outre la difficulté relative à la mise en balance des intérêts en présence et celle relative à l'expression de son opposition, sera donc surtout de pouvoir avoir accès à cette information relative aux modalités d'opposition, notamment lorsque les données ne sont pas collectées directement auprès de lui. Cette problématique se retrouve aussi concernant les modalités d'accès, par l'individu, à ses données.

2. Le droit d'accès

315. L'individu, lorsqu'il fait l'objet d'un traitement de données à caractère personnel, doit également être en mesure de pouvoir accéder aux données le concernant qui sont collectées. L'article 15 du RGPD précise en effet que « la personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ». Ce droit d'accès apparaît ainsi comme étant une modalité d'information *a posteriori* de l'individu. Celui-ci doit pouvoir obtenir du responsable la confirmation que des données à caractère personnel le concernant ont été collectées et disposer ainsi d'un certain nombre de précisions, relatives notamment aux finalités du traitement, aux catégories de données à caractère personnel concernées ou encore aux destinataires de telles données.

316. Un intérêt particulier pour les tiers. Le droit d'accès peut se montrer particulièrement utile en matière d'automesure connectée, notamment pour les cas où les données traitées n'ont pas été collectées directement auprès de la personne concernée. Rappelons l'exemple des *data shadows*[619], lorsque le traitement réalisé permet également d'inclure des données relatives à des tiers, en principe extérieurs au traitement réalisé. L'article 14 du RGPD précise dans ce cas que certaines informations doivent être transmises par le responsable de traitement, à moins que la personne concernée dispose déjà de ces informations. Dans le cas d'une application de *running* qui enregistre les liens d'amitié de la personne, les informations relatives au traitement devront être fournies à la personne concernée par le traitement mais également aux personnes intégrées au cercle d'amis. Rendue illusoire par l'asymétrie informationnelle qui existe entre ces différentes parties, le droit d'accès pourrait servir de correctif permettant à la personne d'avoir confirmation que des données qui la concerne sont traitées, tout en lui permettant de mesurer l'étendue de la collecte réalisée à son sujet.

[619] Cf., *supra*., n° 293.

317. Les risques relatifs au droit d'accès. Les modalités pratiques du recours à ce droit d'accès doivent cependant être repensées, en raison des risques qu'il peut générer. Un magazine allemand a révélé en janvier 2019, postérieurement à l'entrée en application du RGPD, qu'un individu ayant exercé son droit d'accès auprès de la société Amazon pour obtenir les données relatives à une enceinte connectée avait en réalité reçu les fichiers sonores d'une autre personne[620]. Cet incident, qui concernait près de 1700 fichiers, est révélateur des conséquences préjudiciables qu'un droit d'accès mal configuré peut avoir pour les individus. Les fichiers sonores en question pouvaient ici contenir des informations sensibles, telles que des recherches réalisées par suite de l'apparition de certains symptômes. Une situation similaire peut également se présenter en matière d'automesure. Un individu demandant à avoir accès à ses données pourrait ainsi se retrouver en possession des informations d'une autre personne, qu'il s'agisse de ses habitudes alimentaires, relevés d'activités physiques et sexuelles ou données de géolocalisation.

318. Les limites du droit d'accès. La CNIL indique que certaines limites sont applicables au droit d'accès[621], notamment lorsque la demande est infondée ou excessive. La question se pose dès lors de savoir comment apprécier le caractère excessif de la demande d'accès, au regard d'une pratique qui consiste à recueillir un nombre toujours plus important d'informations et ce grâce à des objets connectés. La quantité d'informations collectée pourrait ainsi justifier que des demandes répétées d'accès soient formulées. Outre les frais qui pourraient être demandés à la personne concernée pour l'exercice de ce droit, celui-ci est révélateur de la maîtrise limitée qui est conférée à l'individu sur le traitement réalisé.

§2. La maîtrise limitée du traitement

319. L'article 1er de la LIL prévoit que « toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant ». Ces dispositions ne figurent pas explicitement au sein du RGPD mais

[620] https://www.numerama.com/tech/450138-enceinte-echo-amazon-envoie-par-erreur-1-700-fichiers-sonores-a-la-mauvaise-personne.html?utm_medium=twitter&utm_source=dlvr.it&utm_campaign=450138
[621] https://www.cnil.fr/fr/le-droit-dacces-connaitre-les-donnees-quun-organisme-detient-sur-vous

elles « traduisent la philosophie générale de la réglementation et posent les bases du principe d'autodétermination informationnelle »[622]. Outre la mise en œuvre de principes développés postérieurement tels que le *privacy by design*, cette autodétermination informationnelle doit conduire l'individu à pouvoir maîtriser l'utilisation qui est faite de ses données tout au long du traitement. Des droits qui « ne constituent finalement que la conséquence logique de droits et principes préexistants »[623] lui sont ainsi conférés. Ceux-ci, au titre desquels on retrouve la possibilité pour l'individu de retirer son consentement **(A)**, sont complétés par un droit novateur à la portabilité des données **(B)**.

A. Le droit de retirer son consentement

320. La sanction infligée par la CNIL à Google en janvier 2019 est révélatrice des différents défis portant sur le recueil du consentement de l'individu : information « éclatée dans de multiples endroits avec des niveaux de lecture imbriqués »[624], consentement qui n'est pas univoque ni spécifique ou description des données collectées imprécise et incomplète. Ces griefs, aisément transposables au domaine de l'automesure, confirment que « la volonté est une ressource limitée que l'on peut épuiser ou reconstituer au fil du temps […] surtout dans un monde constamment connecté »[625]. L'individu devrait dès lors être en mesure de recouvrir la pleine maîtrise de sa volonté, que ce soit en retirant celle-ci **(1)** ou en obtenant l'effacement des informations collectées sur ce fondement **(2)**.

1. Le droit au retrait

321. Le consentement de l'individu, préalable nécessaire à l'opération de collecte, doit également perdurer tout au long du traitement qui est mis en œuvre. Le consentement apparaît donc comme un élément nécessaire à la mise en œuvre d'un traitement de données, mais également à sa poursuite. Le principe

[622] Gérard Haas, « Bilan après neuf mois d'application du RGPD », *Dalloz IP/IT*, 2019, p. 357.
[623] Clémence Scottez, « Le RGPD, un nouveau paradigme de la protection des données personnelles pour les professionnels et le régulateur », *Dalloz IP/IT*, 2019, p. 229.
[624] Nathalie Maximin, « Application du RGPD par la CNIL : précisions et amende record pour Google », *Dalloz Actualités*, 28 janvier 2019.
[625] https://www.stanfordlawreview.org/online/privacy-and-big-data-consumer-subject-review-boards/

d'autodétermination informationnelle, bien qu'il ne soit pas consacré explicitement par le texte européen, permet d'expliquer cette nécessité d'un consentement permanent. Celui-ci, en servant de clé de lecture à l'ensemble des dispositions protectrices, vise à l'instauration de principes permettant à l'individu de maîtriser le spectre des informations qu'il dévoile. L'article 7 du RGPD, relatif aux conditions applicables au consentement, indique ainsi que « la personne concernée a le droit de retirer son consentement à tout moment ».

322. Un principe d'équivalence. Ce droit au retrait doit, pour la CNIL, pouvoir être effectué par le biais d'une modalité simple et équivalente à celle utilisée pour recueillir le consentement[626]. Dès lors, un principe d'équivalence des modalités de formulation et de retrait du consentement devrait pouvoir s'appliquer. Or, comme l'indique le RGPD, « lorsque le traitement a plusieurs finalités, le consentement devrait être donné pour l'ensemble d'entre elles »[627]. Ainsi, dans le cas d'une application d'automesure ayant vocation à procéder à un traitement pour des finalités différentes, l'utilisateur devra être en mesure de consentir à chacune des finalités et devra également pouvoir retirer son consentement, indépendamment, pour chacune des finalités exprimées.

Dans le cadre de la pratique de l'automesure connectée, ce droit au retrait se manifestera le plus souvent par l'arrêt de l'utilisation d'un service, par exemple, la désinstallation d'une application. Pourtant, le groupe de l'article 29 insistait dès 2017 dans un avis sur la proposition de règlement ePrivacy[628], sur la nécessité d'interdire les pratiques dites « à prendre ou à laisser », lorsque l'individu doit accepter en bloc les conditions d'utilisation qui lui sont proposées s'il souhaite utiliser un service. Cette absence de négociation des conditions générales d'utilisation, déjà soulevée[629], serait donc susceptible de fausser le consentement de l'individu, mais également d'influencer son retrait. Le considérant 42 du RGPD précise en effet 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

[626] https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes
[627] Considérant 32, Règlement (UE) 2016/79.
[628] G 29, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), wp247, 4 april 2017.
[629] Cf., *supra*, n° 287.

mesure de refuser ou de retirer son consentement sans préjudice ». Selon le parallélisme des formes que doit suivre le retrait du consentement, celui-ci ne serait pas retiré librement si une privation totale des services de l'application en résulte.

323. Un retrait pour l'avenir. Par ailleurs, le retrait du consentement n'a pas vocation à compromettre « la licéité du traitement fondé sur le consentement effectué avant ce retrait »[630]. Celui-ci empêche uniquement la poursuite du traitement pour l'avenir. Dès lors, ce droit au retrait n'implique pas l'effacement des données déjà collectées et traitées par le responsable de traitement. Ne permettant qu'une maîtrise limitée des opérations réalisées sur les données après leur collecte, le droit au retrait du consentement est complété par l'instauration d'un droit à l'effacement communément appelé droit à l'oubli.

2. Le droit à l'oubli

324. Le droit à l'oubli, perçu comme « la prescription des faits qui ne sont plus d'actualité »[631] serait nécessaire dans notre société, au motif que celle-ci « ne peut pas être indéfiniment en colère avec elle-même »[632]. En effet, bien que perçu dans certains cas comme une défaillance de la mémoire, l'oubli serait également « un phénomène vital, un outil de reconstruction psychologique des personnes »[633]. Dès lors, « refuser un droit à l'oubli c'est nourrir l'homme de remords, qui n'a d'autre avenir que son passé, dressé devant lui comme un mur qui bouche l'issue »[634]. Lié au droit de la prescription en ce qu'il constituerait une « prescription du silence »[635], le droit à l'oubli devrait permettre d'éviter aux individus un rappel permanent d'informations, celles-ci pouvant dans certains cas être préjudiciables, notamment pour leur réputation.

---

[630] Article 7, 3, Règlement (UE) 2016/79.
[631] Catherine Costaz, « Le droit à l'oubli », *La Gazette du Palais*, 27 juillet 1995, p. 961.
[632] Paul Ricoeur, *La mémoire, l'histoire, l'oubli*, Paris, Seuil, 2000, 736 p.
[633] Maryline Boizard, « Le temps, le droit à l'oubli et le droit à l'effacement », *Les cahiers de la justice*, 2016, p. 619.
[634] Pierre Kayser, *La protection de la vie privée*, PUAM, 3e éd., 1995, 457 p.
[635] TGI Seine, 4 oct. 1965, JCP 1966 II, 14482, obs. Lyon-Caen.

Inné chez l'être humain en raison de l'écoulement du temps, la nécessité de l'oubli a été confrontée au développement du numérique[636]. En effet, « (...) 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 limite des moteurs de recherche changent considérablement la donne et justifient pleinement qu'un tel droit soit aujourd'hui revendiqué »[637]. La nature des informations en cause permet également de comprendre cette analyse. Données informatiques, celles-ci sont transmissibles, reproductibles à l'infini, non périssables et ne se dégradent pas par l'usage qui en est fait. L'instauration d'un droit à l'oubli, absent de la directive 95/46/CE, a donc eu pour but de limiter les éventuelles conséquences préjudiciables d'activités de traitement de données.

Décriés par certains[638] car il constituerait, entre autres, une atteinte à la liberté d'information[639], le droit à l'oubli numérique a fait son apparition en France, dès 2010, dans deux chartes dénuées de valeur contraignante et visant simplement à sa promotion[640]. Le terme de droit à l'oubli est couramment employé mais il n'a pas vocation à refléter la réalité juridique actuelle. C'est en effet un droit au déréférencement qui a été établi à l'origine, permettant non pas de faire disparaître totalement les informations en cause mais de les désindexer des pages de résultat de moteurs de recherche[641]. Cette solution est celle qui a été retenue par la CJUE en 2014[642] et qui a permis d'ouvrir la voie à un « véritable droit à l'oubli des particuliers, reposant sur le droit au déréférencement »[643]. La Cour avait indiqué que « l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats […] des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne ».

---

[636] Viktor Mayer-Schönberger, *Delete : The Virtue of Forgetting in the Digital Age*, Princeton University Press, 5 juillet 2011, 272 p.
[637] TGI Paris, ord. réf., 25 juin 2009, n° 09/55437.
[638] Jean-Michel Bruguière, « Le « droit à » l'oubli numérique, un droit à oublier », *Recueil Dalloz*, 2014, p. 299.
[639] François Lyn, « Le droit à l'oubli numérique à l'épreuve de la liberté d'information », *AJ pénal*, 2018, p. 462.
[640] Charte du droit à l'oubli numérique dans la publicité ciblée, adoptée le 30 septembre 2010 et Charte du droit à l'oubli numérique dans les sites collaboratifs et moteurs de recherche, adoptée le 13 octobre 2010.
[641] Laure Marino, « Comment mettre en oeuvre le « droit à l'oubli » numérique ? », *Recueil Dalloz*, 2014, p. 1680.
[642] CJUE, 13 mai 2014, aff. C-131/12, *Google Spain c/ Agencia Española de Protección de Datos*.
[643] Conseil d'Etat, *Le Numérique et les droits fondamentaux*, rapport annuel, 2014, p. 184.

325. Des conditions strictes. Novatrice dans son principe, la solution retenue par la Cour a également été appliquée dans l'ordre interne, par le TGI de Paris notamment[644]. La loi pour une République numérique a permis d'en formaliser les termes et d'en déterminer la portée pour les mineurs en complétant la LIL[645] et en ouvrant son exercice à d'autres opérateurs que les seuls moteurs de recherche. Le RGPD, quant à lui, a consacré dans son article 17 un droit à l'effacement pour la personne concernée par un traitement de données. Plusieurs conditions sont exigées par le texte : les données collectées ne doivent plus être nécessaires à réaliser la finalité poursuivie par le traitement, celui-ci était illicite, la personne a retiré son consentement ou s'est opposée au traitement. Ces conditions, relativement strictes, limitent ainsi considérablement la portée de cette disposition.

326. Une opposition entre oubli et bien-être. L'effacement des données est présenté par le texte lui-même comme un « droit à l'oubli ». Celui-ci semble pourtant, plus qu'un véritable droit, n'être qu'une modalité du droit à l'oubli en étant la conséquence d'autres droits qui sont conférés à l'individu. Or, l'étude de ceux-ci, confrontés aux pratiques du *quantified-self*, a permis de relever leur portée limitée face à des techniques de maximisation de collecte des données. Les finalités des applications et dispositifs étant définies largement, la question est posée de savoir comment déterminer que les données collectées ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées. Surtout, la finalité des traitements mis en œuvre dans le cadre de l'automesure étant généralement déterminée en référence au bien-être de l'individu, il s'avère difficile d'établir que celle-ci est atteinte et justifie un effacement des données traitées.

Les difficultés rencontrées pour s'opposer à un traitement ou pour retirer son consentement corroborent ce constat. Consacré au titre des droits de l'individu et non des obligations pesant sur le responsable de traitement, ce droit implique une action positive de l'individu, sans laquelle les données seront conservées. L'individu, ainsi

[644] TGI Paris, ord. Réf. 16 septembre 2014, X et Y., TGI Paris, ord. Réf. 19 décembre 2014, M. et TGI Paris, ord. Réf, 23 mars 2015.
[645] Un article a ainsi été inséré à la loi n°78-17 du 6 janvier 1978, précisant que « sur demande de la personne concernée, le responsable du traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte ».

confronté à un « éléphant numérique qui n'oublie pas facilement »[646] devrait pouvoir, à défaut d'obtenir leur effacement, récupérer les données le concernant.

B. Le droit à la portabilité des données

327. La loi pour une République numérique (LRN) promulguée en octobre 2016, succédant à la loi pour la confiance dans l'économie numérique de 2004, a institué un droit à la portabilité et à la récupération des données. Modifiant le Code de la consommation, l'article 48 de la loi indique que « le consommateur dispose en toutes circonstances d'un droit de récupération de l'ensemble de ses données ». Cette disposition, à portée économique, vise à favoriser la mobilité numérique des utilisateurs de services en ligne tout en évitant les situations « d'enfermement » qui seraient nuisibles à la fois pour la concurrence mais également pour l'essor de nouveaux services innovants[647]. Le droit à la portabilité des données, également consacré à l'article 20 du RGPD, découle du droit à l'autodétermination informationnelle. Novateur dans son principe **(1)**, ce droit a pourtant une portée limitée en matière d'automesure connectée **(2)**.

1. Un droit novateur

328. Le droit à la portabilité des données à caractère personnel est, à plusieurs égards, novateur. D'abord et bien qu'il en soit rapproché, celui-ci doit être distingué du simple droit d'accès aux données à caractère personnel. En effet, déjà mentionné au sein de la directive 95/46/CE, ce droit d'accès ne comporte aucune référence au format dans lequel les données doivent être mises à disposition de la personne concernée par le traitement. Le droit à la portabilité, en revanche, repose sur la transmission, par le responsable de traitement, des données à caractère personnel concernant les individus et ce dans un format structuré, couramment utilisé, lisible par machine et interopérable, afin de pouvoir *in fine* les transmettre à un autre responsable de traitement. Outre l'accès aux données et leur récupération, le droit à la

[646] Nathalie Martial-Braz, Judith Rochfeld, « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? », *Recueil Dalloz*, 2014, p. 1481.
[647] Projet de loi pour une République numérique, Etude d'impact, 9 décembre 2015.

portabilité implique également le droit pour l'individu de transmettre les données à caractère personnel d'un responsable de traitement à un autre. Ces modalités sont confortées par le considérant 68 du RGPD qui précise que le droit à la portabilité des données vise à renforcer le contrôle que les individus exercent sur leurs propres données.

329. Le spectre large de ce droit. Le spectre des données concernées par le droit à la portabilité – données à caractère personnel fournies par la personne – semble en apparence limité. Mais les notions employées font l'objet d'une appréciation large. D'abord, la notion de données à caractère personnel, déjà envisagée, permet d'inclure un nombre très important de données relatives à l'individu[648]. Ensuite, l'emploi du terme « fourni » permet également d'inclure un grand nombre d'informations. Le G29 a par exemple considéré que « pour donner tout son effet à ce nouveau droit, il convient que le terme « fournies » couvre également les données personnelles qui sont observées dans le cadre des activités des utilisateurs, telles que les données brutes traitées par un compteur intelligent ou d'autres types d'objets connectés »[649]. Le droit à la portabilité, selon cette interprétation, concernerait donc les données qui sont délibérément fournies par la personne concernée mais également celles qui sont fournies grâce à l'utilisation du service ou du dispositif, dans le cadre du *quantified-self* par exemple. En prenant l'exemple d'une application de *running*, on constate que la portabilité concerne les données directement renseignées par l'individu lorsqu'il utilise un service : âge, taille ou poids par exemple. Mais elle intègre également les éléments fournis lors de l'utilisation du service : localisation, trajets réalisées ou vitesse. La lecture combinée des deux textes consacrant ce droit, RGPD et LRN, permet de confirmer cette interprétation.

En visant à responsabiliser les personnes concernées pour leur permettre de contrôler davantage les données à caractère personnel les concernant, ce droit a également pour objet d'encourager le développement de services nouveaux dans le

[648] Cf., *supra*, n° 83.
[649] G 29, *Lignes directrices relatives au droit à la portabilité des données*, WP 242, adoptées le 13 décembre 2016, 24 p.

contexte de la stratégie pour un marché unique numérique[650]. Pour y parvenir, l'article 20, 2° du RGPD prévoit une transmission facilitée des données en indiquant que les données à caractère personnel doivent être « transmises directement d'un responsable de traitement à un autre, lorsque cela est techniquement possible ». Cette obligation de moyens qui pèse sur les responsables de traitement doit limiter le manque de compatibilité entre leurs systèmes, au profit d'une interopérabilité renforcée entendue comme « la possibilité de communiquer, d'exécuter des programmes, ou de transférer des données entre diverses unités fonctionnelles d'une façon qui n'exige que peu, voire aucune connaissance des caractéristiques particulières de ces unités de la part de l'utilisateur »[651].

Le droit à la portabilité et à la récupération des données, déjà amorcé pour les fournisseurs de services de communication au public en ligne avec l'adoption de la loi pour une République numérique, voit dès lors sa portée élargie par le RGPD. Cependant, l'application concrète de ce droit au domaine de l'automesure connectée reste limitée.

2. Un droit limité en matière d'automesure

330. En permettant à l'individu de décider de l'usage qui est fait de ses données, la portabilité participerait enfin de son autodétermination informationnelle[652]. Mais le rapport entre autodétermination informationnelle et droit à la portabilité des données doit cependant être tempéré. Initialement introduit dans le dispositif législatif par la loi pour une République numérique du 7 octobre 2016, ce droit soulève un certain paradoxe en ce qu'il semble être ainsi « davantage reconnu dans une perspective commerciale et concurrentielle que dans une perspective de protection de la vie privée de l'individu »[653]. Plusieurs éléments permettraient d'arriver à cette conclusion, parmi lesquels la place qui est faite à cette disposition dans le texte et qui témoignerait de la conception économique de la portabilité. Celle-ci ne figure pas dans la partie de la loi relative à la protection de la vie privée mais

[650] *Ibid.*
[651] Norme ISO/IEC 2382-01.
[652] Charly Berthet, Célia Zolynski, Nicolas Anciaux, Philippe Pucheral, *op. cit.*, p. 29.

dans celle traitant du caractère ouvert de l'environnement numérique. Il serait dès lors davantage question « d'assurer la libre concurrence entre les fournisseurs de services de communications électroniques que de préserver le droit à la vie privée de la personne concernée »[654].

331. L'exclusion des données créées. Transposé au sein du RGPD, ce droit n'a plus seulement une nature économique. Il vise également à protéger les libertés des individus. Pourtant, les restrictions d'application qui lui sont apportées limitent sa portée lorsqu'il est appliqué à des dispositifs d'automesure connectée. Le G29, par son interprétation de la notion de données « fournies par la personne concernée » entend exclure du droit à la portabilité les données déduites et les données dérivées qui sont créées par le responsable du traitement sur la base des données « fournies par la personne », tel que « le résultat d'une appréciation relative à la santé d'un utilisateur »[655]. La CNIL précise cette position en indiquant que les données personnelles qui « sont dérivées, calculées ou inférées à partir des données fournies par la personne concernée, telles que le profil d'un utilisateur créé grâce à l'analyse des données brutes produites par un compteur « intelligent », sont exclues du droit à la portabilité, dans la mesure où elles ne sont pas fournies par la personne concernée, mais créées par l'organisme »[656].

La loi pour une République numérique prévoit déjà cette limite en indiquant l'exclusion du champ du texte les données ayant fait l'objet d'un enrichissement significatif par le fournisseur du service[657]. Celle-ci va cependant plus loin que le texte européen en prévoyant une présomption de non-enrichissement des données. Présomption simple, il s'agit pour les responsables de traitement « de justifier du caractère « significatif » de l'enrichissement, et en quoi la fourniture de données enrichies leur serait préjudiciable »[658]. Cette solution semble aisément compréhensible pour les responsables de traitement. En effet, « les données enrichies

---

[653] Nathalie Martial-Braz, « Les nouveaux droits des individus consacrés par la loi pour une République numérique. Quelles innovations ? Quelle articulation avec le Règlement européen ? », *Dalloz IP/IT*, 2016, p. 525.
[654] *Ibid.*
[655] G 29, *op. cit.*, p. 12.
[656] https://www.cnil.fr/fr/le-droit-la-portabilite-en-questions
[657] Art. L. 224-42-3, al. 1er, 2° du Code de la consommation.
[658] François Pellegrini, « La portabilité des données et des services », *RFAP*, 2018, n° 3, p. 513 à 523.

ne contiennent pas la seule valeur apportée par l'usager, mais un agrégat issu de sources multiples, qu'il pourrait être considéré comme anticoncurrentiel de transmettre à fin de réutilisation par un concurrent »[659]. En excluant ainsi du spectre de la portabilité les données qui résultent d'une analyse du comportement, l'interprétation retenue limite les apports de ce droit pour l'automesure.

Le principe propre au fonctionnement du *quantified-self* repose sur l'enrichissement significatif systématique des données produites à partir de l'activité d'un individu. Dès lors, seul un nombre limité de données serait susceptible d'être concerné par la portabilité, à l'image du poids ou de la taille renseignés par une personne configurant une application de *running*, ou du rythme cardiaque enregistré lors d'un effort physique. Les investissements réalisés par les développeurs de dispositifs pour configurer leurs produits justifient que les processus de personnalisation des services soient exclus du droit à la portabilité. L'application de la portabilité à l'automesure, limitée *in fine* à la récupération d'un nombre restreint d'informations, conduirait également à amoindrir la portabilité des services et le nombre de transferts directs entre responsables de traitement.

332. Le droit à la portabilité des services. Le droit à la portabilité des services, qui consiste en la possibilité de faire transférer les données directement d'un prestataire à un autre, est justifié par le fait que « peu de personnes disposent des compétences leur permettant de manipuler elles-mêmes les masses de données qui leur sont transmises »[660]. L'individu doit dès lors pouvoir changer facilement de prestataire et celui-ci est chargé d'y contribuer en procédant lui-même au transfert. Pourtant, « dans le monde des services numériques, chaque acteur se différencie souvent des autres par un positionnement et des services distincts de ses concurrents » et « une portabilité permettant aux personnes de retrouver à l'identique l'ensemble des services est donc difficilement envisageable »[661]. L'hypothèse d'un individu souhaitant récupérer ses données d'une application de *running* pour les transférer sur un autre service semble difficilement imaginable et le fait qu'un service procède directement à ce transfert l'est également.

[659] *Ibid.*

333. La question du coût de sortie. Par ailleurs, la dimension sociale de ces applications, fondée sur le partage d'informations à des cercles de tiers déterminés par l'individu, complexifie cette portabilité des services. Le « coût « de sortie », lié à la mise à disposition des modules et interfaces de programmation permettant l'exportation des données »[662] se double ainsi d'un coût de rentrée qui impliquera notamment d'obtenir le consentement des tiers éventuellement concernés par le traitement initial. Le considérant 68 du RGPD précise en effet que « lorsque, dans un ensemble de données à caractère personnel, plusieurs personnes sont concernées, le droit de recevoir les données à caractère personnel devrait s'entendre sans préjudice des droits et libertés des autres personnes concernées conformément au présent règlement ». Le second responsable de traitement devra alors recueillir le consentement des tiers éventuellement concernés par le traitement afin, selon l'article 20, 4°, de ne pas porter atteinte à leurs droits et libertés. Il est possible de reprendre ici l'exemple déjà mentionné d'une application de *running* relevant les liens d'amitié de l'utilisateur. Si ce dernier décide d'exercer son droit à la portabilité, le second responsable de traitement, destinataire des données, devra également recueillir le consentement des « amis ».

Le droit à la portabilité découle, par la récupération des données qu'il implique, du droit d'accès. Mais il n'en constitue qu'une modalité renforcée ne permettant pas de participer véritablement, pour l'utilisateur d'un dispositif de *quantified-self*, à son autodétermination informationnelle. L'encadrement limité du traitement de données sensibles ne permet également pas de répondre aux nombreuses difficultés d'application pratiques de ce droit.

SECTION II. L'ENCADREMENT LIMITÉ DU TRAITEMENT

334. Les données sensibles susceptibles d'être collectées afin de faire l'objet d'un traitement sont, dans le cadre du *quantified-self*, nombreuses et variées. Des

---

[660] *Ibid.*
[661] *Ibid.*
[662] *Ibid.*

données relatives à l'apparence[663], à la consonnance des noms et prénoms, susceptibles de révéler l'origine des individus[664] ou encore à la vie sexuelle[665] peuvent être intégrées au spectre des données collectées. Les traitements mis en œuvre sont également susceptibles de révéler, directement ou indirectement, des informations qui sont relatives à la santé de l'individu. Cette notion de donnée de santé, qui fait l'objet d'une interprétation large par la jurisprudence, est désormais clairement définie par le RGPD.

335. Le traitement des données sensibles est en principe interdit par la réglementation. La loi française, par la transposition de la directive de 1995, a consacré cette interdiction dès 2004. Celle-ci, par suite d'une réécriture du texte postérieure à l'adoption du RGPD, figure désormais au sein de l'article 6 et concerne les données à caractère personnel « qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter 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 ». Cette interdiction, également mentionnée à l'article 9 du règlement, présente un spectre large dont la portée doit être tempérée **(Paragraphe 1)** en raison des garanties supplémentaires qui sont théoriquement apportées aux traitements réalisés **(Paragraphe 2)**.

§1. Une autorisation de traitement limitée

336. L'article 9 du RGPD, outre une énumération des données considérées comme sensibles ou « particulières » selon le texte, pose un principe d'interdiction du traitement de telles données. Cette interdiction, justifiée par le caractère particulièrement intime des informations en question, doit cependant être relativisée. Le texte prévoit en effet une liste limitative d'exceptions permettant de procéder à un

[663] CNIL, Délibération n° 2007-006 du 18 janvier 2007.
[664] CNIL, Délibération n° 96-105 du 3 décembre 1996.
[665] CNIL, Délibération n° 02-012 du 14 mars 2002.

traitement de données sensibles. La possibilité limitée de traiter ces données repose sur une précision des conditions de licéité de tels traitements **(A)** et suppose, dans certains cas, que des formalités supplémentaires soient réalisées **(B)**.

A. Les conditions de licéité précisées

337. La condition relative à la licéité du traitement n'est pas propre à ceux portant sur des données sensibles. L'article 6 du RGPD fait de la licéité du traitement un principe général de validité de la collecte de données. Le consentement de l'individu figure parmi ces conditions et procéder à un traitement sans l'avoir recueilli est puni par des dispositions du Code pénal[666]. En matière de catégories particulières de données à caractère personnel, le consentement présente un rôle renouvelé. Outre une condition de licéité du traitement, celui-ci permet de lever l'interdiction de principe du traitement de données sensibles. Explicite **(1)**, celui-ci porte sur des catégories de données qui auront éventuellement vocation à faire l'objet d'un hébergement sécurisé **(2)**.

1. Un consentement explicite

338. Déjà requises pour la mise en œuvre d'un traitement de données personnelles classiques, certaines garanties nécessaires à la mise en œuvre d'opérations de collecte sont renforcées pour le traitement de données sensibles. L'article 8 de la loi du 6 janvier 1978, telle que modifiée par la loi de transposition de la directive, en 2004, indiquait déjà que n'étaient pas soumis à l'interdiction de principe les traitements pour lesquels la personne concernée avait donné son « consentement exprès ». Le consentement requis pour le traitement de données sensibles devait donc présenter une intensité renforcée, justifiée par la nature particulière des données collectées. Relativement vague quant à son acception, la notion de consentement exprès a fait l'objet d'interprétations différentes.

[666] Art. 226-16 du Code pénal : « Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende ».

339. Une notion évolutive. Le Conseil d'Etat adoptait, avant 2004, une approche relativement stricte de la notion. Selon lui, la seule information accordée à la personne ne permettait pas de retenir la notion d'accord exprès[667]. La CNIL se montrait également stricte puisqu'elle considérait que l'accord devait être nécessairement écrit et présenté sur un document distinct du formulaire de collecte[668]. Ainsi, le fait pour un individu de savoir que des données le concernant allaient être intégrées à un fichier ne suffisait pas à caractériser l'accord exprès requis par le texte. Cette position, partagée par la CJUE, réfutait l'idée que l'accord puisse être implicite[669]. La CNIL a eu l'occasion de réaffirmer que le consentement exprès s'entend d'un accord explicite et écrit[670]. Mais certaines de ses délibérations, préalablement à l'entrée en vigueur du RGPD, ont montré que celle-ci peut également faire preuve de souplesse[671], justifiée par des considérations pratiques relatives à la nécessité de traiter des données.

340. Une condition confirmée par le RGPD. Le RGPD, ayant pour certains la volonté d'unifier les règles relatives au consentement[672], confirme la nécessité d'obtenir un consentement renforcé. Le consentement requis dans le cadre de l'article 9 du RGPD, auquel la LIL fait également référence, doit ainsi être explicite et donné pour une ou plusieurs finalités spécifiques. Le terme explicite se rapporte ici à la façon dont le consentement est exprimé par la personne concernée et une manière évidente de s'assurer que le consentement est explicite serait, entre autres, « de confirmer expressément le consentement dans une déclaration écrite »[673]. Toutefois, la pratique de l'automesure connectée soulève certaines interrogations, en dépit de ces exigences relatives à l'obtention d'un consentement renforcé.

341. Des difficultés pratiques. Certaines de ces interrogations ne sont pas propres au traitement des données sensibles et ont déjà été envisagée à propos de la

---

[667] CE, 5 juin 1987, *Kaberseli*, n° 59674, Lebon, p. 205.
[668] CNIL, *8ème rapport d'activité 1987*, La Documentation française, 1988, p. 17 et p. 28.
[669] CJUE, Gr. Ch., 9 novembre 2010, Affaires jointes C-92/09 et C-93/09 *Volker und Markus Schecke GbR et Hartmut Eifert contre Land Hessen*, §64.
[670] CNIL, Défenseur des droits, *Mesurer pour progresser vers l'égalité des chances*, Guide méthodologique à l'usage des acteurs de l'emploi, 2012, p. 16.
[671] CNIL, Délibération n°2007-106 du 15 mai 2007 ; CNIL, Délibération n°2010-449 du 2 décembre 2010.
[672] Estelle Brosset, « Le droit à l'épreuve de la e-santé : quelle « connexion » du droit de l'Union européenne ? », *RDSS*, 2016, p. 869.
[673] G29, *Lignes directrices sur le consentement au sens du règlement 2016/679*, WP 259, adoptées le 28 novembre 2017, version révisée et adoptée le 10 avril 2018.

liberté que doit revêtir le don du consentement. Dans certains cas, cette liberté est remise en question lorsque le traitement intervient « contractuellement comme pré-condition à l'utilisation de certains appareils, services ou applications ou dès lors que certains appareils connectés seraient offerts gratuitement à condition que leurs utilisateurs consentent à la collecte et au traitement des données personnelles captées par ces appareils »[674]. Affaiblie par cette conditionnalité, la portée du consentement l'est par le fait que celui-ci doit être donné en lien avec « une ou plusieurs finalités spécifiques ».

L'individu devrait en effet, face à des engagements de confidentialité, pouvoir consentir à chacune des finalités avancées : finalités relatives au traitement de données personnelles d'une part et finalités relatives au traitement de données sensibles d'autre part. L'étude d'un certain nombre de conditions générales d'utilisation montre pourtant que cette faculté ne lui est pas offerte, étant donné qu'aucune différence n'est réalisée entre le traitement portant sur des données personnelles et celui portant sur des données sensibles. Procéder à un hébergement sécurisé de telles données pourrait dans certains cas servir de correctif *ex post* à un traitement de données sensibles mais l'obligation de procéder à une telle sécurisation de l'hébergement reste limitée.

2. Un hébergement sécurisé

342. Une garantie justifiée par la nature des données traitées. Les données de santé ne sont pas des données sensibles comme les autres. Celles-ci, en raison des informations qu'elles révèlent et de leur éventuel regroupement au sein de bases de données médico-administratives, font l'objet de garanties supplémentaires au titre desquelles figure l'hébergement sécurisé. L'article L. 1111-8 du Code de la santé publique donne ainsi un cadre à l'hébergement des données de santé à caractère personnel. Ces données peuvent, depuis 2002 et la loi Kouchner, être déposées auprès

[674] Antoinette Rouvroy, *Des données et des hommes. Droits et libertés fondamentaux dans un monde de données massives*, Rapport à destination du Comité Consultatif de la Convention pour la protection des personnes au regard du traitement automatisé de données personnelles du Conseil de l'Europe, 2015, p. 29.

d'une personne physique ou morale agréée à cet effet[675]. Parfois intitulé « coffre-fort numérique »[676], le dispositif d'hébergement mis en place vise à renforcer la protection accordée aux données de santé traitées à l'occasion d'activités de prévention, de diagnostic ou de soins ou de suivi social et médico-social.

Complétée par un décret de janvier 2006 pris après avis de la CNIL[677], la procédure repose sur un agrément par le ministre de la santé après dépôt d'un dossier à l'ASIP santé, le recueil d'un avis de la CNIL et d'un comité d'agrément des hébergeurs placés auprès du ministre. Cette faculté, qui vise à assurer la sécurité, la confidentialité et la disponibilité des données de santé lorsque leur hébergement est externalisé, a également été remaniée par la loi du 26 janvier 2016 qui a ajouté au texte la référence aux activités de suivi-social et médico-social. La loi de 2016 étend la portée de l'hébergement au secteur social et les conditions de mise en œuvre de cet hébergement, modifiées, reposent désormais sur une procédure de certification. Certains points particuliers, tels que les mesures de sécurité prises pour éviter toute violation du secret médical ou encore la traçabilité des accès et le chiffrement des transmissions, font l'objet d'une évaluation et d'une appréciation avant que la demande d'agrément soit jugée recevable[678].

343. Une garantie inadaptée à l'automesure. L'énoncé de ces conditions, également précisé par un guide commun entre la CNIL et l'Ordre des médecins[679], montre qu'utilisés en complément d'un parcours traditionnel de soins, les données issues d'objets connectés et applications de *quantified-self* utilisés en santé pourraient être soumises à un hébergement sécurisé. L'ASIP santé fournit sur son site une liste des hébergeurs agréés et parmi ceux-ci, on peut retrouver les opérateurs qui le sont « pour une prestation d'hébergement de données de santé à caractère personnel collectées au moyen d'application fournies par les clients ». Pourtant, la complexité des démarches à entreprendre révèle l'inadéquation de ce cadre protecteur aux

[675] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.
[676] Isabelle Vacarie, « L'hébergement des données de santé : entre contrat et statut », *RDSS*, 2002, p. 695.
[677] Sur ce point, voir : CNIL, Délibération n°2004-041 du 27 mai 2004 et Délibération n°2005-045 du 15 mars 2005.
[678] Voir par exemple sur ce point : CNIL, délibération du 4 avril 2013, par laquelle est autorisée l'expérimentation pendant une durée de deux ans d'une messagerie sécurisée de santé mise en place par l'ASIP santé pour encourager les professionnels de santé à n'échanger des données de santé que par courriels sécurisés.
[679] CNIL et Conseil National de l'Ordre des médecins, *Guide pratique sur la protection des données personnelles*, Edition juin 2018, p. 9.

dispositifs de *quantified-self* utilisés dans un cadre ludique ou sportif, quand bien même ils procéderaient à une collecte incidente de données de santé. Ainsi, la majeure partie des données sensibles relatives à la santé collectées dans le cadre de l'automesure n'auront pas vocation, outre les dispositions relatives aux mesures de sécurité à mettre en œuvre de l'article 32 du RGPD tels que la pseudonymisation ou le chiffrement, à faire l'objet d'un hébergement sécurisé et agréé.

B. Les formalités renouvelées

344. La mise en œuvre d'un traitement de données à caractère personnel devait, antérieurement à l'adoption du RGPD, respecter certaines formalités visant à protéger l'individu et ses données. Reposant sur la déclaration préalable et la demande d'autorisation, toutes deux formulées auprès de la CNIL, ce régime devait permettre une maîtrise des opérations de collecte réalisées. Pourtant, la pertinence de ces mécanismes a été remise en cause par le développement de dispositifs permettant de procéder à une collecte importante et instantanée de données. Aujourd'hui abandonnée **(1)**, ces formalités ont tout de même permis de poser les fondements de certains principes protecteurs, ce qui explique leur survivance dans certaines hypothèses **(2)**.

1. L'abandon des formalités préalables

345. La LIL, dans sa version initiale telle que publiée au Journal officiel du 7 janvier 1978, prévoyait que les traitements automatisés d'informations nominatives devaient faire l'objet d'une déclaration auprès de la CNIL, en échange de quoi un récépissé était délivré au responsable de traitement. Certains auteurs voyaient cette déclaration comme « une forme allégée d'autorisation préalable »[680] et le Conseil d'Etat a eu l'occasion de montrer les limites du refus de délivrance du récépissé[681]. La

[680] Didier Chauvaux, Thierry-Xavier Girardot, « Régime de la déclaration préalable des traitements informatisés d'informations nominatives », *AJDA*, 1997, p. 156.

[681] Le Conseil d'Etat considère sur ce point que, « s'il appartient à la Commission nationale de l'informatique et des libertés de s'assurer de la régularité de la déclaration effectuée auprès d'elle au regard des prescriptions des articles 16 et 19 précités, et notamment de ce que les précisions exigées par l'article 19 figurent dans la déclaration, il résulte des termes mêmes de l'article 16 que la commission ou son président ne peut refuser de délivrer récépissé du dépôt de déclaration, dès lors que le dossier présenté comporte bien l'engagement prévu à l'article 16 précité et est conforme aux prescriptions de l'article 19 précité ». CE, 6 janvier 1997, *Caisse d'épargne Rhône Alpes Lyon*, 159129, publié au recueil Lebon.

réforme du droit à la protection des données à caractère personnel, amorcée par la directive de 1995, a permis la consécration d'un changement de paradigme dans la mise en œuvre des formalités préalables au traitement de données et la loi du 6 août 2004 a fait de la déclaration préalable le régime de droit commun.

346. Des formalités inadaptées. Cette harmonisation du régime déclaratif n'a pourtant pas permis d'en renforcer la pertinence, à l'heure de la généralisation des traitements massifs de données. La LIL prévoyait elle-même des cas dans lesquels les traitements n'étaient soumis à aucune formalité préalable[682]. Par ailleurs, la CNIL pouvait également définir, parmi les catégories les plus courantes de traitements et dont la mise en œuvre n'était pas susceptible de porter atteinte à la vie privée, des dispenses à l'obligation de déclaration. A cette dispense, fondée sur les finalités, destinataires, catégories de destinataires des données traitées ou durée de conservation de celles-ci, s'ajoutait également des déclarations simplifiées pour les catégories les plus courantes de traitements de données.

Le RGPD ne reprend pas à son compte les dispositions relatives à l'obligation de déclaration des traitements de données personnelles. Celui-ci acte en effet le passage d'une logique déclarative des traitements mis en œuvre à la CNIL à une logique de responsabilisation des acteurs chargés de traiter des données. Ce changement de paradigme doit notamment être expliqué au regard des capacités de traitement de données désormais mises en œuvre par les objets connectés utilisés pour la pratique de l'automesure. Le flot continu d'informations collectées rend en effet inutile le recours à des formalités préalables permettant d'identifier les opérations réalisées. Celles-ci étant désormais nombreuses et surtout instantanées, prévoir en amont les traitements mis en œuvre ne permet plus d'assurer leur visibilité. Pourtant, dans certaines hypothèses, ces formalités sont maintenues et doivent permettre une protection accrue des traitements portant sur des données sensibles.

[682] Béatrice Guillaume, « Dispense, déclarations ou autorisation : la nature des données fait la différence », *JA*, 2007, n° 357, p. 13.

2. La survivance des formalités administratives

347. La LIL réécrite présente, dans une section 3 relative aux traitements de données à caractère personnel dans le domaine de la santé, des dispositions plus précises que celles du RGPD et qui permettent de le compléter. Selon l'article 66 de la loi, les traitements réalisés dans le domaine de la santé, en considération de la finalité d'intérêt public qu'ils présentent, ne peuvent être mis en œuvre que dans deux cas de figure. Ceux-ci doivent d'abord être traitées conformément à des référentiels et règlements types, établis par la CNIL en concertation avec l'Institut National des données de santé (INDS) devenu, avec la loi du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé, le groupement d'intérêt public « Plateforme des données de santé ». Lorsque les traitements mis en œuvre sont conformes à ces référentiels, une déclaration doit être adressée par le responsable de traitement à la CNIL, attestant de cette conformité. En revanche, lorsque les traitements ne sont pas conformes aux instruments précités, le mécanisme de l'autorisation par la CNIL est conservé et la demande formulée doit, en vertu de l'article 33 du texte, mentionner certains éléments : identité du responsable de traitement, finalité ou encore éventuelles interconnexions.

348. La finalité d'intérêt public. Les traitements de données à caractère personnel qui sont réalisés dans le domaine de la santé et qui sont concernés par ces mécanismes de conformité à des référentiels ou d'autorisation doivent avoir une finalité d'intérêt public. Ces formalités préalables maintenues par la loi s'apparentent dès lors à « une « soupape » de droit souple […] qui garantissent une évolution et adaptation au contexte technologique et sociétal »[683]. Mais l'interprétation de la notion d'intérêt public à laquelle le texte fait référence, porteuse d'incertitudes, devrait pourtant conduire à écarter la majorité des dispositifs d'automesure du cadre protecteur qui est ici exposé. L'article 66 du texte indique que la garantie de normes élevées de qualité et de sécurité des dispositifs médicaux constitue une finalité d'intérêt public. Mais comme cela a déjà été montré, la majorité des dispositifs d'automesure échappe à cette catégorie[684] et les traitements qu'ils permettent de

[683] Elise Debiès, « Big data de santé et autodétermination informationnelle », *RFAP*, n° 167, 2018, p. 570.
[684] Cf., *supra*, n° 183.

réaliser s'opéreront en dehors du cadre des formalités administratives toujours mobilisées.

§2. Des garanties renforcées

349. Le RGPD ainsi que la LIL réécrite présentent un cadre général de protection des données sensibles, fondé sur la force renouvelée du consentement de l'individu. Ce cadre est par ailleurs complété par un ensemble de dispositions qui sont spécifiquement applicables à une catégorie particulière de données sensibles : les données de santé. Leur collecte et leur manipulation sont aujourd'hui un enjeu majeur de la transformation de nos systèmes de santé et ces données doivent permettre, à terme, le développement d'une santé fondée sur la prédiction et la prévention. En effet, l'individu ou patient potentiel prend, avec ses données, une part de plus en plus active dans la gestion de sa santé[685]. Il devient ainsi cocréateur de parcours de soins et contribue, grâce à l'innovation, à la modernisation de la décision publique en santé.

Fondée sur une politique de prévention des risques, l'action des individus doit donc contribuer au renforcement de la démocratie en santé[686]. Initié par une disposition de la loi du 4 mars 2002 selon laquelle le patient prend, « avec le professionnel de santé et compte tenu des informations et des préconisations qu'il lui fournit, les décisions concernant sa santé »[687], ce renforcement du rôle des individus pourrait être facilité par l'exploitation des données issues de l'automesure. Le cadre juridique applicable aux données qui en sont issues est cependant révélateur des limites du rapprochement entre santé et dispositifs de *quantified-self*. Justifié par la finalité spécifique qui lui est conférée **(A)**, le cadre juridique protecteur des données de santé est *de facto* susceptible de limiter l'apport du *quantified-self* au domaine sanitaire **(B)**.

---

[685] François Pellegrini, « L'utilisation des données à caractère personnel dans le cadre de la personnalisation des traitements », *in* Cécile Castaing (dir.), *Technologies médicales innovantes et protection des droits fondamentaux des patients*, mare & martin, 2017, p. 105.
[686] Danièle Cristol, « L'usager dans la stratégie nationale de santé : la démocratie en santé en quête d'un nouveau souffle », *RDSS*, 2018, p. 413.
[687] Art. L. 1111-4, CSP.

A. Une finalité spécifique

350. Le principe d'interdiction de la collecte et du traitement des données personnelles sensibles contenu à l'article 9 du RGPD fait l'objet d'un certain nombre de dérogations. Celles-ci, précisées au fil de l'évolution des textes, permettent la mise en œuvre de traitements portant sur des données sensibles. Explicitement consacrées par la loi, ces dérogations reposaient avant sa réécriture sur la finalité du traitement. Cette référence a aujourd'hui disparu mais les exceptions à l'interdiction de traiter des données sensibles ayant vocation à s'appliquer dans le cadre du *quantified-self* restent les mêmes. Celles-ci sont notamment relatives à l'exercice de la médecine **(1)** ainsi qu'à l'amélioration des systèmes de santé **(2)**.

1. L'exercice de la médecine

351. Les liens entre automesure et santé. La pratique de l'automesure connectée entretient aujourd'hui des liens étroits avec le domaine médical. Les applications et dispositifs mis en œuvre ont de plus en plus tendance à s'insérer au sein d'un parcours de soin traditionnel et d'un écosystème global de santé connectée[688]. Les traitements courants mis en œuvre par les médecins et le personnel soignant font partie des exceptions consacrées par le texte. L'ancien article 8 de la LIL précisait ainsi que « les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose, en raison de ses fonctions, l'obligation de secret professionnel prévue par l'article 226-13 du Code pénal » ne faisaient pas l'objet d'une interdiction de traitement.

352. Une exception justifiée par le secret professionnel. Le nouvel article 6 du texte reprend en substance cette exception, par renvoi à l'article 9 du RGPD qui mentionne la question des diagnostics médicaux et de la prise en charge sanitaire ou

[688] Commission Européenne, *La Santé en poche : libérer le potentiel de la santé mobile*, Communiqué de Presse, Bruxelles, le 10 avril 2014.

sociale. Cet article fait également référence au secret professionnel[689]. En effet, ces dérogations, justifiées par le besoin pour les professionnels de santé de mettre en œuvre des traitements de données personnelles relatifs à leurs patients, sont légitimés par le recours au secret professionnel. Cet élément, déjà pris en compte par la CNIL sous l'empire de la LIL telle qu'elle résultait de la transposition de la directive de 1995, avait d'ailleurs fait l'objet d'une norme simplifiée fixant les conditions de mise en œuvre de tels traitements[690], complétée par une autorisation unique en vue d'encadrer l'échange de données à caractère personnel de santé entre professionnels[691]. Cette possibilité qui est laissée de déroger à l'interdiction de principe du traitement des données sensibles est ainsi en grande partie justifiée par le fait que ces données se trouvent traitées par une catégorie de personnes soumise au secret professionnel.

Partagés entre les différents professionnels participant à la prise en charge d'une même personne, ce secret vise à garantir le droit au respect de la vie privée de la personne et le secret des informations la concernant[692]. Le Code pénal indique, en contrepartie, qu'est incriminé le fait pour une personne « dépositaire d'une information à caractère secret, soit par état, soit par profession, soit en raison d'une fonction ou d'une mission temporaire, de révéler cette information »[693]. Un dispositif d'automesure connectée utilisé dans un cadre médical doit donc pouvoir bénéficier de la dérogation permettant de légitimer le traitement de données sensibles, à la condition que les données soient manipulées par une personne soumise au secret.

353. Cette notion de secret, qui apparaît également « en filigrane de la protection des données de santé devant la Cour européenne des droits de

[689] L'article 9, 3° du Règlement européen indique en effet que « les données à caractère personnel […] peuvent faire l'objet d'un traitement […] si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel ».
[690] Délibération n°2005-296 du 22 novembre 2005, portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les membres des professions médicales et paramédicales exerçant à titre libéral à des fins de gestion de leur cabinet.
[691] CNIL, délibération n° 2014-239 du 12 juin 2014, portant autorisation unique de mise en œuvre, par les professionnels et établissements de santé ainsi que par les professionnels du secteur médico-social habilités par une loi, de traitements de données à caractère personnel ayant pour finalité l'échange par voie électronique de données de santé à travers un système de messagerie sécurisée.
[692] Art. L. 1110-4 du CSP.
[693] Art. 226-13 du Code pénal.

l'homme »[694], est mentionné par la recommandation n° R (97) 5 du Comité des ministres du Conseil de l'Europe, relative à la protection des données médicales. Ce document explicite le fait que la collecte et le traitement de données de santé ne peuvent être réalisées, en raison de leur caractère sensible, que par des « professionnels des soins de santé » ou des « personnes ou organismes agissant pour le compte de professionnels des soins de santé » et qui doivent être « soumis aux règles de confidentialité propres aux professionnels de santé ».

Le secret professionnel apparaît donc comme une garantie permettant le traitement de données sensibles[695]. Il s'applique dans des hypothèses limitées au cadre du *quantified-self*, en raison des intérêts que celui-ci peut présenter pour la recherche dans le domaine de la santé.

2. La recherche en santé

354. La loi Informatique et Libertés, avant sa réécriture, indiquait que les traitements nécessaires à la recherche, aux études et évaluations dans le domaine de santé n'étaient pas soumis à l'interdiction de principe des données sensibles. Cette dérogation n'était pourtant pas présente dans la directive de 1995 puisqu'elle n'entrait pas « dans le cadre des traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé mentionnés par le texte »[696]. Sa consécration dans la loi a eu pour objet de donner « une base légale aux communications de données à caractère personnel nécessaires à la constitution de fichiers de recherche en permettant, sous certaines conditions, une levée du secret professionnel »[697].

355. L'exception à l'interdiction de traiter des données sensibles, lorsqu'elle permet la mise en œuvre de traitements courants, repose sur la garantie offerte par le secret professionnel et dépend donc du statut des personnes appelées à collecter de

[694] Sophie Gambardella, « Une lecture de la jurisprudence de la Cour européenne des droits de l'Homme relative aux données de santé », *RDSS*, 2016, p. 271.
[695] Alexis Déroudille, « Le secret professionnel dans le règlement général sur la protection des données », *RFDA*, 2018, p. 1112.
[696] Anne Debet, Jean Massot, Nathalie Metallinos, *Informatique et Libertés, La protection des données à caractère personnel en droit français et européen*, Lextenso éditions, 2015, p. 409.
[697] Jeanne Bossi, « Comment organiser aujourd'hui en France la protection des données de santé ? », *RDSS*, 2010, p. 208.

telles données. Les traitements qui sont réalisés à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé repose, quant à eux, sur une finalité d'intérêt public. Dans ce cadre, ils doivent être précédés de la mise en place de référentiels, règlements types ou à défaut, demandes d'autorisation[698] et sont donc fondés sur un encadrement spécifique de l'opération de traitement. Pourtant, l'irruption du bien-être dans la santé, selon la définition qui en est donnée par l'OMS, ainsi que les nouveaux modes de collecte et de traitement des données de santé, notamment à partir d'objets connectés, font que « nous nous trouvons ainsi aujourd'hui à la croisée des chemins »[699]. Les objets connectés utilisés pour la pratique de l'automesure n'ont pas vocation à remplacer le médecin généraliste, « mais l'enjeu actuel réside dans la capacité à inventer des modèles pour intégrer la nouvelle data dans la pratique médicale »[700].

356. L'*evidence based medicine*. La rigueur du cadre juridique applicable aux données de santé traitées en milieu médical ou pour la recherche est aisément compréhensible. Celle-ci repose sur la collecte et le traitement de données à vocation scientifique, suivant le modèle de l'*evidence based medicine*[701]. Plusieurs éléments permettent d'envisager une sorte de présomption de fiabilité des données collectées. L'arrêt Mercier de la Cour de cassation indiquait déjà, en 1936, qu'il se forme « entre le médecin et son client un véritable contrat comportant, pour le praticien, l'engagement, sinon, bien évidemment, de guérir le malade, ce qui n'a d'ailleurs jamais été allégué, du moins de lui donner des soins, non pas quelconques […], mais consciencieux, attentifs et, réserve faite de circonstances exceptionnelles, conformes aux données acquises de la science »[702]. Le Code de déontologie médicale de l'Ordre des médecins dispose quant à lui, à propos du diagnostic, que celui-ci doit être élaboré par le médecin « avec le plus grand soin, en y consacrant le temps nécessaire,

[698] Cf., *supra*, n° 349.
[699] Elise Debiès, « L'ouverture et la réutilisation des données de santé : panorama et enjeux », *RDSS*, 2016, p. 697.
[700] *Ibid*.
[701] Thomas Lauvin, *« Evidence-Based Medicine », quelle place dans la décision du médecin ?*, Thèse d'exercice en médecine générale, Université Toulouse III-Paul Sabatier, soutenue le 2 juillet 2013.
[702] Cass. Civ., 20 mai 1936, *Mercier* ; *RTD civ*. 1936. 691, obs. Demogue ; GAJC, 12e éd., 2008, n° 162-163.

en s'aidant dans toute la mesure du possible des méthodes scientifiques les mieux adaptées »[703].

357. Le problème de la fiabilité des mesures. Le problème est que les objets connectés utilisés pour la pratique de l'automesure, dont le fonctionnement repose sur une collecte importante de données afin d'en dégager des tendances et des évolutions, posent parfois certains doutes quant à leur fiabilité, comme a pu le relever la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF)[704]. La publication de référentiel de bonnes pratiques devrait permettre, à terme, une fiabilité renforcée des applications et objets dans le domaine de la santé[705]. Mais ceux-ci n'ont cependant pas vocation, pour l'heure, à délivrer les mêmes diagnostics qu'un médecin, ce que de nombreuses applications explicitent d'ailleurs. L'équipementier sportif Under Armour précise par exemple :

> *« Tout le contenu proposé par les Services, qu'il soit fourni par nous, par d'autres utilisateurs ou par des tiers (même s'ils prétendent être médecins), n'est pas destiné à être et ne doit pas être utilisé en remplacement de l'avis de votre médecin ou d'autres professionnels de la santé, une visite, un appel ou une consultation avec votre médecin ou d'autres professionnels de la santé […] Votre utilisation des Services ne constitue ni ne crée de relation professionnelle docteur-patient, thérapeute-patient ou autre relation professionnelle de santé entre Under Armour et vous.*[706].

Les tendances qui sont dégagées par l'analyse de grands ensembles de données ne présentent donc pas le même rôle qu'une consultation médicale. Mais ces tendances peuvent pourtant contribuer au développement d'une santé à deux vitesses,

[703] Art. R. 4127-33, CSP.
[704] https://www.economie.gouv.fr/dgccrf/objets-connectes-sante-et-bien-etre-sont-ils-fiables
[705] Haute Autorité de Santé, *Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (Mobile Health ou mHealth)*, octobre 2016, 60 p.
[706] https://account.underarmour.com/fr-fr/terms-and-conditions#

santé empirique dans un cadre médico-administratif d'une part et santé fondée sur l'analyse du *big data* d'autre part[707].

358. Le risque d'une santé à deux vitesses. L'innovation en santé, telle qu'elle est notamment prônée par la Stratégie nationale de santé 2018-2022[708], devrait conduire à « réaffirmer la place des usagers dans la transformation du système de santé et restaurer leur confiance dans le traitement de leurs données personnelles ou collectives »[709]. Le retard dans l'intégration du numérique en santé et dans son cadre juridique fait aujourd'hui l'objet d'efforts de modernisation[710]. L'article 45 de la loi de santé adoptée en juillet 2019 prévoit la création d'un « Espace numérique de santé » ouvert automatiquement[711]. Cet espace, accessible en ligne et opérationnel au plus tard en janvier 2022, permettra à son titulaire d'accéder à ses données administratives, à son dossier médical partagé mais également à « ses constantes de santé éventuellement produites par des applications ou des objets connectés »[712]. Les conditions d'alimentation de l'espace numérique de santé par des données issues de ces dispositifs restent encore à préciser. En tout état de cause, ces services devront faire l'objet d'un référencement et respecter des référentiels d'interopérabilité et de sécurité, des labels et des normes établis notamment par le groupement d'intérêt public « Plateforme des données de santé », successeur de l'INDS.

En dépit du manque de précisions de ces dispositions, d'éventuels retards dans la mise en œuvre de ce dispositif pourraient conduire à renforcer les inégalités de santé et à remettre en cause l'égal accès aux soins[713] à l'heure ou de nouveaux services numériques se développent, tel que le protocole Watson développé par IBM qui permet la réalisation de diagnostics automatisés par la corrélation d'informations provenant de sources différentes. La rigueur du cadre juridique applicable aux données de santé n'a pas vocation à s'appliquer systématiquement aux dispositifs d'automesure, montrant par la même occasion l'intégration limitée de celle-ci au

[707] Clémentine Lequillerier, « « L'ubérisation » de la santé », *Dalloz IP/IT*, 2017, p. 155.
[708] Ministère des solidarités et de la santé, *Stratégie nationale de santé 2018-2022*, p. 66.
[709] Danièle Bourcier, Primavera de Filippi, « Vers un droit collectif sur les données de santé », *RDSS*, 2018, p. 444.
[710] Florence Eon, « L'accélération du numérique en santé : enjeux et conditions de son succès », *RDSS*, 2019, p. 55.
[711] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé.
[712] Article L. 111-13-1 du Code de la santé publique, version à venir au 1er janvier 2022.
[713] Brigitte Feuillet, « L'accès aux soins, entre promesse et réalité », *RDSS*, 2008, p. 713.

domaine de la santé. Les modalités de réutilisation de telles informations, également encadrée, sont susceptibles de limiter l'apport du *quantified-self* au domaine sanitaire.

B. L'apport limité de l'automesure au domaine sanitaire

359. Le cadre juridique protecteur qui est applicable aux données de santé montre, par sa rigueur, que les dispositifs d'automesure en sont généralement exclus. Ceux-ci, utilisés avec le consentement de l'individu dans un cadre majoritairement ludique ou sportif, ne sont pas encore tout à fait intégrés au domaine de la santé. Ils y font surtout des incursions temporaires que le droit peine à maîtriser et que les pouvoirs publics ont du mal à exploiter dans la mise en œuvre renouvelée de politiques de santé. Par ailleurs, les responsables de traitement, parfois de jeunes *start-ups* aux capacités financières de recherche et de développement limitées, ne sont pas en mesure de maîtriser précisément le cadre juridique applicable. Dès lors, la complexité croissante du droit de la protection des données personnelles **(1)** conduit également à une limitation des possibilités de réutilisation des informations collectées dans le cadre de l'automesure **(2)**.

1. La complexité du cadre juridique

360. Les nouvelles dispositions relatives aux données et plus particulièrement aux données de santé, témoignent de la complexité croissante du droit des données à caractère personnel. Les itérations successives de la loi Informatique et Libertés, bien qu'elles aient pour but de procéder à l'adaptation du cadre juridique national aux dispositions européennes, conduisent en effet à un manque de lisibilité globale des dispositions applicables. Les nombreux renvois au texte européen, ainsi qu'à d'autres dispositions contenues dans la loi, empêchent les responsables de traitement d'avoir une vue d'ensemble des démarches à effectuer pour agir en conformité et garantir aux individus leur autodétermination informationnelle. Par ailleurs, en matière de santé, le régime applicable aux données ne relève pas uniquement de la loi Informatique et Libertés mais concerne plus généralement les dispositions sur le secret[714], sur la

[714] Art. L. 1110-4, CSP.

sécurité et l'interopérabilité[715], l'hébergement[716] ou la mise à disposition[717] qui relèvent du Code de la santé publique.

361. Un cadre en pleine mutation. L'article 32 de la loi du 20 juin 2018, portant adaptation du cadre juridique national aux dispositions du Règlement européen[718], a habilité le gouvernement à passer par voie d'ordonnance pour procéder à la réécriture de « l'ensemble de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés afin d'apporter les corrections formelles et les adaptations nécessaires à la simplification et à la cohérence ainsi qu'à la simplicité de la mise en œuvre par les personnes concernées des dispositions qui mettent le droit national en conformité avec le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ». Pourtant, comme le révèlent certains auteurs[719], ce procédé semble manquer de cohérence et celui-ci soulève différentes questions relatives à la complexité du dispositif mis en œuvre.

362. Un frein à l'automesure. Le Conseil constitutionnel, saisi de la question[720], a eu l'occasion d'écarter les griefs tenant au défaut d'accessibilité et d'intelligibilité de la loi[721]. Pourtant, cette absence de clarté du dispositif protecteur en matière de données à caractère personnel et en matière de protection des données sensibles constitue un frein important à l'usage qui pourrait être fait des données collectées en matière d'automesure. Celles-ci sont en effet susceptibles de présenter un fort intérêt en matière sanitaire, social ou médical. L'œuvre graphique réalisée par l'artiste Marcin Ignac, à partir de données à caractère personnel, semble particulièrement révélatrice de ces apports. Le père de l'artiste ayant été victime d'un accident de voiture, celui-ci lui a fait parvenir un bracelet connecté, *tracker d'activité*, afin de pouvoir suivre l'évolution de sa convalescence. L'expérience, réalisée sur cinq semaines, a permis de montrer les différentes phases de récupération de l'individu à la suite de l'accident. Ce projet s'inscrivait dans le cadre d'une

[715] Art. L. 1110-4-1 du CSP.
[716] Art. L. 1111-8 et R. 1111-8 s. du CSP.
[717] Art. L. 1460-1 s. du CSP.
[718] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, article 32.
[719] Voir notamment : Nathalie Martial-Braz, « L'abus de textes peut-il nuire à l'efficacité du droit ? », *Dalloz IP/IT*, 2018, p. 459.
[720] CC, décision n° 2018-765 DC du 12 juin 2018, *Loi relative à la protection des données personnelles*.
[721] Jean-Marc Pastor, « Constitution, loi et règlement européen : mode d'emploi », *AJDA*, 2018, p. 1191.

démarche artistique fondée sur l'utilisation des données[722] et dont les résultats ont été présenté à la fondation EDF au cours de l'été 2018[723].

De telles démarches pourraient également être adoptées dans le domaine médical afin de suivre au mieux les différents stades de guérison, suite notamment à des fractures. La difficulté à déterminer avec précision le régime applicable aux données personnelles sensibles est dès lors susceptible de limiter ce type d'apports et par la même occasion d'en limiter les possibilités de réutilisation.

2. Des modalités de réutilisation limitées

363. L'exploitation des données de santé représente un « matériel essentiel de la recherche en santé »[724] qui devrait à terme entraîner le bouleversement du système de santé tel qu'il est pensé et fonctionne à l'heure actuelle[725]. L'enjeu des politiques publiques en santé est en effet de promouvoir l'accès aux données ouvertes à la réutilisation : c'est-à-dire, « au-delà de l'accès à l'information qu'elles constituent, leur usage pour constituer des bases de connaissances et réaliser des services utiles aux consommateurs, aux collectivités, aux marketeurs, aux innovateurs et aux contributeurs citoyens de toutes sortes »[726]. L'Etat développe depuis 1978 et l'adoption de la loi « CADA »[727] une politique d'ouverture et de partage des données publiques visant à assurer une certaine forme de transparence[728]. Celle-ci s'insère aujourd'hui plus globalement dans un mouvement d'*open data* visant à la réutilisation des informations libérées[729].

364. La réutilisation des données libérées. Le but recherché lors de l'ouverture des données publiques, particulièrement celles relatives à la santé, réside dans la possibilité pour tout un chacun de s'approprier et de réutiliser ces données

[722] http://marcinignac.com/projects/quantified-other/
[723] https://fondation.edf.com/fr/expositions/1-2-3
[724] Rapport de la Commission Open Data en santé, remis à Madame Marisol Touraine, ministre des Affaires sociales et de la santé, le 9 juillet 2014, p. 44.
[725] Renaissance Numérique, *D'un système de santé curatif à un modèle préventif grâce aux outils du numérique – 16 propositions pour un changement de paradigme des politiques de santé*, Livre blanc rédigé sous la direction d'Henri Isaac, septembre 2014.
[726] Cerema, « L'open Data en collectivité à la lumière des données de mobilités », *Centre d'études et d'expertise sur les risques, l'environnement, la mobilité et l'aménagement*, mars 2015, p. 5.
[727] Loi n° 78-753 du 17 juillet 1978.
[728] Pour plus de précisions sur la notion et ses évolutions, voir : RFAP, *Données publiques*, ENA, n°167, 282 p.

afin de développer de nouveaux services. Signe que le rapport à la santé est en train de subir une mutation profonde[730], cette ouverture des données en vue de leur réutilisation doit constituer une méthode alternative économiquement viable face à l'augmentation du coût des soins[731]. L'enjeu relatif à l'ouverture et aux modalités de réutilisation des données est, à l'égard de l'automesure et des dispositifs qui sont utilisés, double. D'une part, est posée la question de la possibilité d'alimenter les bases de données soumises à ouverture par des données issues de l'automesure. D'autre part, est posée celle de la réutilisation des données libérées par des fournisseurs de service d'automesure afin d'améliorer leurs prestations.

365. Dans le premier cas, la nature des données collectées ainsi que leur contexte de création doivent conduire à écarter l'hypothèse selon laquelle celles-ci pourraient véritablement alimenter les bases de données médico-administratives soumises à ouverture. Le système national de données de santé (SNDS) qui est créé afin de procéder à une ouverture maîtrisée des données de santé est alimenté par les données de différentes bases médico-administratives telles que le Système national d'information inter-régimes de l'Assurance maladie (SNIIRAM). Les données collectées par des responsables de traitement dans le domaine de l'automesure connectée n'ont pas, pour l'heure, vocation à y figurer et les données d'automesure n'ont pas vocation à être libérées à des fins de réutilisation.

La loi pour une République numérique a consacré la notion de données d'intérêt général mais celle-ci, bien que pouvant concourir à une conduite plus efficace de politiques publiques sectorielles, n'a pas vocation à s'appliquer aux opérateurs d'automesure. L'analyse juridique conduit en effet à penser que « la majorité des ensembles de données traités par les entreprises dans le cadre de leur activité relèvent du droit de propriété : soit au titre du droit *sui generis*, soit en tant qu'actif incorporel »[732].

---

[729] Art. L. 312-1 du CRPA.
[730] Gilles Babinet, *L'ère numérique, un nouvel âge de l'humanité*, Le Passeur, 2014, 236 p.
[731] CNNum, *La santé, bien commun de la société numérique*, Rapport remis à la Ministre des Affaires sociales, de la Santé et des Droits des femmes, La Documentation française, octobre 2015, 128 p.
[732] Rapport Conseil d'Etat / CGE / IGF, *Rapport relatif aux données d'intérêt général*, septembre 2015, 93 p.

366. Dans le second cas, la question posée est celle de la possibilité de réutilisation, par des prestataires de services d'automesure, des données issues de bases médico-administratives. En effet, les données médico-administratives sont susceptibles de présenter un intérêt pour la qualité des applications d'automesure qui se développent sur le marché. L'article L. 1460-1 du Code de la santé publique issu de la loi de modernisation de notre système de santé de 2016 prévoit cette possibilité[733] . La transmission des données de santé de l'assurance maladie aux *start-ups*, aux chercheurs et aux scientifiques afin d'identifier de nouveaux besoins de santé, de nouvelles relations de cause à effet et de trouver de nouveaux champs d'innovation doit ici se faire dans le strict respect de l'anonymat[734] et la réutilisation de ces données ne peut avoir ni pour objet ni pour effet d'identifier les personnes concernées[735]. Le principe de l'*open data* en santé nécessite ainsi qu'un juste équilibre soit trouvé entre les bénéfices d'une mise à disposition des données et la sauvegarde de la vie privée des individus[736]. L'article 193 de la loi de modernisation du système de santé du 26 janvier 2016 apporte ainsi certaines limites à la réutilisation des données issues du SNDS.

La complexité du cadre juridique actuel, qui a notamment mené la CNIL et la CADA à publier un guide pratique sur la présentation du cadre juridique de l'*open data*[737], limite pourtant les hypothèses d'ouverture et de réutilisation des données de santé. Les développeurs d'applications et dispositifs de *quantified-self* ne seraient dès lors pas en mesure de profiter pleinement de cette ouverture pour procéder à l'amélioration de leurs services. Ces éléments de réflexion sur la pertinence du cadre juridique, appliqués aux données de santé, sont également révélateurs de la prise en compte limitée de l'automesure par le droit.

---

[733] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.
[734] Marisol Touraine, présentation en lecture définitive du projet de loi de modernisation de notre système de santé à l'Assemblée nationale le 17 décembre 2015.
[735] Lydia Morlet-Haïdara, « Le système national des données de santé et le nouveau régime d'accès aux données », *RDSS*, 2018, p. 91
[736] Pour une présentation complète des modalités d'accès aux données : Jeanne Bossi Malafosse, « Les nouvelles règles d'accès aux bases médico-administratives », *Dalloz IP/IT*, 2016, p. 205.
[737] CNIL et CADA, *Guide pratique de la publication en ligne et de la réutilisation des données publiques (« open data »)*, Présentation du cadre juridique de l'ouverture des données, Document élaboré par les services de la CADA et de la CNIL en association avec les services d'Etalab, février 2019, 21 p.

367. Conclusion du chapitre. Le traitement de données à caractère personnel est en principe libre et s'inscrit, au niveau européen, dans une perspective de libre-échange de l'information entre Etats membres. En contrepartie de cette liberté, les responsables de traitement doivent respecter un certain nombre d'obligations tout en garantissant que les individus puissent exercer leurs droits. Deux éléments permettent cependant de montrer en quoi le dispositif protecteur, confronté à la pratique de l'automesure, présente certaines limites. D'abord, l'information parcellaire délivrée à l'individu lors de la mise en œuvre d'un traitement ne lui permet pas d'avoir une vue d'ensemble des moyens dont il dispose pour maîtriser ses données. Ensuite, ses droits se révèlent en pratique limités face aux capacités techniques des dispositifs utilisés : le nombre d'informations collectées et la permanence des opérations de collecte rendent complexe toute tentative de maîtrise *ex post*. Le régime juridique applicable aux données de santé produites en contexte médical aurait pu, dans certains cas, apporter des garanties supplémentaires. Mais le rattachement encore limité du domaine de l'automesure à celui de la santé fait que ces garanties n'ont pas entièrement vocation à s'appliquer, révélant l'insuffisance des principes protecteurs contenus au sein de la règlementation.

368. Conclusion du titre. Les données issues de dispositifs d'automesure connectées font aujourd'hui l'objet d'une protection limitée : le régime juridique en place a en effet du mal à saisir dans sa globalité les problématiques soulevées par le *quantified-self*. Ce dernier favorise, par son fonctionnement, la dissémination croissante de données de natures différentes et soumises à des régimes juridiques distincts. Ce faisant, le *quantified-self* contribue non seulement à une remise en cause des catégories juridiques de données établies par la loi mais il rend également complexe l'idée d'une maîtrise par les individus des flux de données qu'ils contribuent à créer. La portée limitée du droit à l'oubli confirme cette hypothèse, à deux niveaux différents. D'une part, la masse d'information créée est susceptible de rendre illusoire toute tentative de maîtrise, *a posteriori*, des informations révélées. D'autre part, la finalité de l'automesure, relative à l'évolution de constantes relatives au bien-être, s'oppose en principe à ce que des données soient effacées. L'exemple topique du droit à l'oubli est révélateur des limites de la réglementation face à une pratique visant à favoriser la révélation de l'intimité.

369. Conclusion de la partie. La pratique du *quantified-self* permet de mettre en lumière les limites de la réglementation. Le droit à la protection des données est en effet confronté à une pratique qui cumule différents services numériques et qui contribue à l'accroissement exponentiel du nombre de données à caractère personnel collectées et traitées. Cette remise en question de la pertinence du cadre juridique est aggravée par le rapport ambigu que le *quantified-self* entretient avec le domaine de la santé. Utilisés principalement dans un cadre ludique, les dispositifs d'automesure font des incursions dans le domaine de la santé que le droit peine à saisir. Cette ambiguïté du lien avec le domaine sanitaire est renforcée par la capacité des dispositifs utilisés à pouvoir révéler des éléments relatifs à la santé, même lorsqu'ils sont uniquement mobilisés dans un cadre purement ludique.

L'adoption du RGPD a permis de révéler, au sein des entreprises, certaines problématiques relatives à la gouvernance des données traitées. En effet, beaucoup de responsables de traitement n'avaient pas connaissance, avant le renouveau du cadre juridique européen, des obligations à leur charge. La fragilisation de la protection, en plus de cette méconnaissance des règles, s'est également opérée par le recours à des principes protecteurs pouvant sembler dépassés, au regard des capacités de collecte des dispositifs utilisés. Le phénomène du *big data*, associé à une logique de valorisation des données par les entreprises, est ainsi venu restreindre la portée des droits conférés aux individus. La convergence de ces différents éléments, au moment où le *quantified-self* a été largement adopté par le grand public, a contribué au délitement du cadre juridique protecteur. Ainsi fragilisé, le droit à la protection des données a dû faire l'objet, plutôt que de simples réaménagements, d'une véritable reconstruction.

DEUXIÈME PARTIE – LA RECONSTRUCTION DU CADRE JURIDIQUE

370. Le cadre juridique relatif à la protection des données à caractère personnel, aujourd'hui fragilisé par le développement de nouveaux outils de collecte à grande échelle, a été amené à faire l'objet d'une réforme d'ampleur avec l'adoption du Règlement général européen sur la protection des données. Celui-ci, adopté en avril 2016 et entré en application le 25 mai 2018, procède à une révolution copernicienne des modalités de mise en œuvre des traitements de données, notamment par l'abandon de nombreuses formalités préalables. Certains mécanismes de protection, que l'on pourrait qualifier de « statiques », ont été conservés après l'entrée en application du RGPD : principe de finalité déterminée, de proportionnalité du traitement ou de durée de conservation limitée des données. Ceux-ci, devant être respectés par tout responsable de traitement, sont particulièrement exposés au développement de l'automesure. Mais plusieurs outils « dynamiques » de protection ont progressivement été déployés, préfigurant dans certains cas les dispositions du nouveau texte européen.

371. Imaginés par les autorités nationales de protection des données, des instruments tels que les analyses d'impact relatives à la vie privée ou les règles d'entreprise contraignantes sont révélateurs de la technicité croissante du droit à la protection des données à caractère personnel. En s'inscrivant dans le domaine de la régulation, envisagée comme une « normativité dialoguée »[738], ces instruments permettent d'attester de la création d'un droit protecteur des données « à la carte », en fonction des spécificités de chacun des traitements mis en œuvre. Certaines problématiques, relatives par exemple à la distinction entre données personnelles et données personnelles sensibles, ont ainsi tendance à s'effacer pour laisser place à la

[738] Gérard Timsit, « Normativité et régulation », *Cahiers du Conseil constitutionnel*, n° 21, Études et doctrines, La normativité.

mise en œuvre d'un dispositif protecteur créé sur mesure par les responsables de traitement, en fonction des spécificités des opérations réalisées. Les nouveaux mécanismes consacrés par le RGPD doivent dès lors permettre leur meilleure prise en compte.

372. Les éléments de réglementation majoritairement figés qui étaient mis en place par la directive 95/46/CE, tout en étant maintenus, sont complétés par des éléments de régulation plus souples et mieux adaptés aux spécificités des traitements mis en œuvre. La notion de régulation, que l'on peut définir comme « une fonction de la puissance publique qui tend à établir un compromis entre des objectifs et des valeurs économiques et non économiques »[739], a été « très longtemps ignorée des juristes »[740]. Celle-ci, opposée à la réglementation rigide[741], vise à faire en sorte « qu'un système complexe puisse se maintenir durablement dans un état d'équilibre dynamique, par le jeu de rétroactions internes et d'actions de contrôle externes »[742]. La régulation, co-construite par le législateur et par les acteurs du secteur, permettrait ainsi, par sa souplesse, une meilleure maîtrise des risques engendrés par les nouveaux moyens de collecte et de traitement des données à caractère personnel. Surtout, contrôlée par les autorités administratives qui participent également à son élaboration[743], la régulation apporterait une réponse adaptée aux spécificités de chaque situation, ce qu'une règle de droit figée et fixant des principes *a priori* ne serait pas toujours en mesure de favoriser.

Le principe de neutralité technologique, qui irriguait déjà la formulation des principes contenues au sein de la directive de 1995 et de la loi Informatique et Libertés modifiée, est désormais explicitement consacré par le RGPD. Sa mise en œuvre concrète repose sur la formulation large des termes employés par la réglementation et par la prise en compte des opérations de collecte, sans considération des innovations technologiques employées. Cette généralité des termes utilisés est également le socle permettant à la régulation de se développer. Les

[739] Gérard Marcou, « La notion juridique de régulation », *AJDA*, 2006, p. 347.
[740] Karine Favro, *Droit de la régulation des communications numériques*, LGDJ, coll. Systèmes, 2018, p. 7.
[741] Gérard Timsit, « La loi et ses doubles. Thématiques du raisonnement juridique », *Droits*, n°36, 2002, p. 160.
[742] Nicolas Curien, Géraldine Pflierger, « La régulation des communications électroniques en Europe », *Flux*, n° 87, 2012/1, p.86.

principes généraux instaurés par le cadre renouvelé de protection sont ainsi complétés, en fonction des spécificités de chaque traitement et de chaque secteur, par des éléments de régulation plus précis et mieux adaptés. Ainsi, la mise en œuvre d'un cadre juridique large a favorisé la prise en compte des évolutions techniques utilisées pour la pratique de l'automesure **(Titre I)**, tout en contribuant au développement d'une nouvelle forme de régulation du traitement des données à caractère personnel **(Titre II)**.

[743] Catherine Teitgen-Colly, « Les autorités administratives indépendantes : histoire d'une institution », *in* Colliard C.-A et Timsit G. (dir.), *Les autorités administratives indépendantes*, PUF, 1998, p. 26.

TITRE I – LA PRISE EN COMPTE DES ÉVOLUTIONS TECHNIQUES PAR UN CADRE JURIDIQUE LARGE

373. Le *quantified-self*, ainsi que les objets connectés utilisés pour sa pratique, repose sur l'utilisation de canaux de collecte et de traitement déjà connus et déjà employés. Mais la principale novation, qui a notamment une influence sur la qualification des données qui sont collectées, est la multiplication des possibilités de recueil d'informations, favorisée par le déploiement de ces nouveaux instruments de collecte et de traitement des données. En effet, la spécificité de l'Internet des objets consiste en une capacité de dialogue et d'échange renouvelés d'informations entre différents médias dans l'optique de bénéficier d'une analyse toujours plus poussée des informations collectées. Une donnée, par nature volatile, est dès lors susceptible d'être stockée hors des instruments utilisés pour la collecte et peut également faire l'objet de transferts instantanés entre plusieurs supports informationnels, situés en différents emplacements géographiques.

Les mécanismes d'automesure connectée, en faisant appel à divers dispositifs (généralement au moins un objet connecté ou un *smartphone* relié à une application), permettent en effet la mise en œuvre de chaînes de traitement de données. Celles-ci, découlant des différentes évolutions de la technologie et rendues possibles par la connexion à Internet d'objets du quotidien, questionnent dans certains cas la pertinence de la règlementation. En effet, ces chaînes de traitement reposent d'abord sur un transfert quasi-constant des informations collectées, les données recueillies dans le cadre de l'automesure n'ayant pas vocation à être statiques, mais à être transférées à de nombreuses reprises. Ensuite, en raison des capacités de stockage parfois limitées des instruments utilisées, les données ont vocation à faire l'objet, après leur collecte, de différentes analyses et comparaisons. A ce titre, les fournisseurs de services mettant à disposition les objets connectés ne seront pas forcément ceux qui procèderont ensuite à l'analyse des informations collectées.

374. L'externalisation des différentes opérations de traitement n'est pas née directement de la miniaturisation des objets utilisés pour la pratique de l'automesure. Des transferts de données avaient déjà lieu auparavant et l'absence de frontières terrestres dans le cyberespace permettait déjà que des données fassent l'objet de transferts entre différents responsables de traitement situés en différentes localisations géographiques. Mais la diminution du coût de stockage et du coût de la puissance de calcul des ordinateurs ont rendu courantes ces externalisations qui font désormais partie du modèle de traitement des données personnelles. Les capacités renforcées de croisement de données ont confirmé la pérennité de ce modèle de traitement reposant sur l'échange et l'externalisation des différentes opérations réalisées. La législation n'intégrait à l'origine pas ces questions mais ses évolutions progressives ont pourtant eu tendance à permettre un encadrement de ces externalisations. Un cadre juridique large, non tributaire des instruments techniques utilisés et donc technologiquement neutre a *in fine* été adopté, permettant une prise en compte des externalisations structurelles **(chapitre 1)** et géographiques **(chapitre 2)** sur lesquelles reposent les outils d'automesure connectée.

CHAPITRE I – LA PRISE EN COMPTE DES EXTERNALISATIONS STRUCTURELLES

375. Le *quantified-self* était à l'origine réalisé manuellement et il consistait, pour son pratiquant, à noter des éléments de manière répétée[744]. Mais son automatisation a permis le développement d'une chaîne d'opérateurs appelés à participer à la collecte et au traitement de telles données. L'automesure, tout en permettant la création de données personnelles relatives à différentes activités – économiques, physiques, sportives ou encore sanitaires – implique généralement que ces mêmes données, relatives à un individu, fassent l'objet d'un transfert presque constant entre différents acteurs qui participent à l'écosystème de *quantified-self*[745]. En effet, l'automatisation et la connexion des services utilisés implique majoritairement le recours à d'autres acteurs, fournisseurs de services, qui vont permettre de mener à bien cette automatisation et cette numérisation du *quantified-self*.

376. L'individu souhaitant procéder à une automesure peut toujours mesurer seul son activité physique. Pourtant, il dispose désormais de différents outils technologiques pour y procéder, objets du quotidien connecté à Internet dans le cadre de l'IoT qui communiquent avec l'utilisateur ou directement entre eux, augmentant par la même occasion les flux de données qui en sont issus[746]. La technologie RFID (*Radio Frequency Identification*), qui consiste en l'intégration d'une puce électronique intelligente dans un objet, permet de rendre les dispositifs d'automesure opérationnels et celle-ci a notamment pour but de permettre leur « communication avec un lecteur chargé de recevoir des informations »[747]. Cette interconnexion de différents supports capables de collecter des données personnelles est l'élément

[744] CNIL, *Lettre Innovation et Prospective*, n° 5, juillet 2013, p. 2.
[745] Synthèse de l'AFCDP sur le Quantified-self connecté, *op. cit.*, p. 10.
[746] Commission des Communautés européennes, Communication de la commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, *L'Internet des objets – un plan d'action pour l'Europe*, Bruxelles, 18 juin 2006, COM (2009)278 final, p. 2.
[747] Gérard Haas, Amanda Dubarry, Marie D'Auvergne, Rachel Ruimy, « Enjeux et réalités juridiques des Objets Connectés », *Dalloz IP/IT*, 2016, p. 394.

central de cet écosystème de *quantified-self*. Elle permet en effet un partage grandissant d'informations entre différentes plateformes : objets connectés du quotidien (pèse-personnes, brosses à dents), *trackers* d'activités, *smartphones*, tablettes et ordinateurs. Ceux-ci communiquent dès lors entre eux et se transmettent mutuellement des données identifiantes et potentiellement sensibles. Un système de mesure pouvant servir à relever une information et à transformer l'activité physique en donnée informatique peut dès lors être couplé à un logiciel permettant de traiter les données mesurées.

L'individu pourra d'abord avoir recours à une application directement installée sur un smartphone, une tablette ou tout autre terminal mobile tel un *tracker* d'activité. Dans ce cas, si la collecte et l'analyse par l'application ont lieu au sein du même instrument, le fabricant de l'objet utilisé pourra différer du fournisseur de l'application. De même, les données pourront être conservées en dehors du dispositif, par un prestataire de *cloud-computing*. Ensuite, l'individu pourra utiliser des capteurs installés au sein d'objets connectés qui transmettront ces données à d'autres applications, installées sur un support mobile différent. Enfin, les données collectées pourront également être directement collectées, analysées et stockées par les constructeurs ou encore transmises à des tierces parties, qu'il s'agisse de réseaux sociaux, de communautés dédiées ou encore d'acteurs du monde médical. Une logique de plateforme pourra également être développée, visant à l'adoption par les utilisateurs de services additionnels[748].

377. Cette multiplication des acteurs est susceptible de perturber l'application de la réglementation protectrice des données personnelles. En effet, le nombre croissant d'opérateurs à même de manipuler les données relatives aux individus est susceptible d'influencer la lisibilité des textes en question et surtout de nuire à la clarté des obligations pesant sur les différentes parties impliquées. Les définitions qui étaient contenues dans la précédente version de la loi Informatique et Libertés et qui ont été précisées par le RGPD ont cependant vocation à montrer la portée élargie du texte. Celui-ci permet « d'aborder l'ensemble des problèmes que pose l'utilisation de

[748] Mehdi Nemri, *Demain, l'Internet des objets*, Commissariat général à la stratégie et à la prospective, France Stratégie, Note d'Analyse, janvier 2015, n°22, p. 3.

l'informatique au regard de toutes les libertés, quel que soit l'organisme concerné (public ou privé) et quels que soient les objectifs poursuivis par l'informatisation »[749]. Cette volonté de ne pas faire dépendre la réglementation des évolutions technologiques permet notamment une adéquation des principes de protection à une collecte et à un traitement de données dont « le volume, la variété et la vélocité » ne peuvent que croître[750]. L'architecture décentralisée des différents traitements de données réalisés dans le cadre du *quantified-self* **(section 1)** impose un encadrement renouvelé des capacités de réutilisation des données personnelles des individus **(section 2)**.

[749] Ariane Mole, « Au-delà de la loi informatique et libertés », *Droit social*, Dalloz, 1992, p. 603.
[750] Conseil économique, social et environnement, *Les données numériques : un enjeu d'éducation et de citoyenneté*, avis présenté par M. Éric Peres, rapporteur au nom de la section de l'éducation, de la culture et de la communication, 2015, p. 12.

SECTION I – LES RISQUES D'UNE ARCHITECTURE DECENTRALISÉE

378. Le *quantified-self* a pour particularité d'instaurer une véritable chaîne d'opérateurs dans le traitement des données de l'individu. Ce dernier en est la pièce centrale mais l'automesure connectée contribue pourtant à décentraliser les données qui lui sont rattachées. En effet, chacune des étapes principales – collecte, analyse, stockage – peut être réalisée par un tiers. Ces différentes étapes permettent à l'individu de bénéficier d'une analyse renforcée de son activité. Ainsi, les données collectées dans le cadre du *quantified-self* ont de plus en plus vocation à être externalisées **(Paragraphe 1)** mais cette externalisation fait l'objet d'un certain nombre de garanties visant à assurer la sécurité des données en question **(Paragraphe 2)**.

§1. Une gestion externalisée

379. La loi Informatique et Libertés énonce en son article premier que les individus doivent pouvoir décider et contrôler les usages qui sont faits des données à caractère personnel les concernant. L'ensemble de la réglementation relative à la protection des données personnelles vise en effet à atteindre cet objectif d'autodétermination informationnelle et son accomplissement repose en grande partie sur l'identification de la personne responsable du traitement de données à caractère personnel. L'enjeu relatif à cette identification est en effet essentiel, puisque le rattachement des obligations dont le responsable de traitement a la charge en découle.

Cette tâche relative à l'identification peut pourtant se révéler délicate étant donné les différents acteurs qui sont appelés à intervenir dans la délivrance d'un service de *quantified-self*. La chaîne d'acteurs et d'opérateurs nécessite en effet d'être décomposée afin d'identifier d'abord et à titre principal la personne responsable du traitement de données personnelles **(A)**, bien que l'architecture propre aux dispositifs de *quantified-self* implique également d'aborder, à titre incident, la qualification de sous-traitant **(B)**.

A. La qualification principale de responsable de traitement

380. L'application des principes protecteurs contenus dans la loi Informatique et Libertés et dans le RGPD – relatifs notamment à la responsabilité – suppose d'identifier de manière préalable le responsable du traitement de données. A l'origine du ou des traitements mis en œuvre, il est en effet normal qu'il soit chargé d'assumer la responsabilité des opérations réalisées. Pourtant, la diversité des acteurs susceptibles d'intervenir dans la mise en œuvre d'un dispositif de *quantified-self* rend son identification parfois complexe **(1)** même si celle-ci n'est pas exclusive et peut justifier qu'un régime de coresponsabilité soit dans certains cas retenu **(2)**.

1. Une qualification complexe en raison de la multiplication du nombre d'acteurs

381. L'évolution de la notion. La loi Informatique et Libertés ne faisait à l'origine aucune référence à la notion de responsable de traitement. Ce dernier apparaissait simplement en filigrane dans le texte, mentionné par exemple au sein de l'ancien article 19 comme étant celui ayant le pouvoir de décider de la création d'un traitement de donnée et donc, de présenter la demande d'avis ou de déclaration dudit traitement à la CNIL. La version initiale de la loi faisait également référence en son article 29 à la personne « ordonnant un traitement d'informations nominatives » et la CNIL en avait ainsi déduit que c'est à elle que revenait la tâche de signer le formulaire de déclaration du traitement[751].

Dès 1981 cependant, la notion a été matérialisée au sein de l'article 2 de la Convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel. Intitulé à l'origine « maître du fichier », le responsable de traitement était ainsi « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées ». Surtout, c'est à cette notion que la CNIL,

[751] Sénat, rapport n°218, *op. cit.*, 19 mars 2003, p. 50.

la jurisprudence et la doctrine avaient l'occasion de faire référence dans leurs différents travaux[752].

L'intitulé de la fonction n'a pas été directement repris selon les mêmes termes par la suite et la directive de 1995 a développé, à travers la notion de « responsable de traitement », un titre correspondant à des responsabilités similaires. Alors que la référence à la détermination de la finalité par « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme » a été maintenue, la détermination des moyens du traitement de données à caractère personnel est venue s'ajouter à la détermination de la finalité d'un tel traitement. Essentiellement inspirée de la Convention 108, la définition proposée a donc été transposée à l'article 3 de la loi Informatique et Libertés. Celle-ci employait jusqu'en 2003 le terme de « responsable de fichier » et la terminologie a finalement été modifiée pour traiter du « responsable de traitement ».

382. L'importance de la notion. Ainsi, la version actualisée de la loi fait également du responsable de traitement « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement »[753]. Cette détermination des finalités et des moyens apparaît donc comme le critère central permettant l'identification précise du responsable de traitement et *in fine* de la personne chargée de faire respecter les règles de protection des données. En effet, l'ensemble des dispositions relatives aux droits de l'individu, qu'il s'agisse par exemple du droit d'information[754], d'accès ou encore d'opposition, a pour point de rattachement la personne concernée d'une part, mais également le responsable de traitement d'autre part. La possibilité pour les personnes concernées de faire exercer leurs droits ainsi que la détermination du droit national applicable dépendent de l'identification du responsable de traitement.

---

[752] Pascal Ancel, « La protection des données personnelles : aspects de droit privé français », *RICD*, 1987, vol. 39, n°3, p. 611.
[753] La loi Informatique et Libertés, dans sa version antérieure, définissait directement la notion de responsable de traitement. Celle-ci, par suite de sa réécriture par l'ordonnance du 12 décembre 2018, renvoie désormais directement à la définition adoptée à l'article 4 du Règlement européen.
[754] CE, 23 mars 2015, n° 357556.

383. Un critère cumulatif. La loi de 2004, en transposant la directive de 1995, a proposé une définition du responsable de traitement fondée sur un critère cumulatif de détermination des moyens mais également des finalités du traitement. Son identification, réalisée grâce à des critères qui ont été repris par le RGPD, semble en apparence simple. Pourtant, celle-ci est confrontée, dans le cadre du *quantified-self* notamment, à la présence de plusieurs intervenants qui rendent difficile l'identification certaine de la personne en charge de déterminer les deux critères précités. Le G29, dans un avis rendu en 2010, a précisé la méthodologie permettant de déterminer avec certitude l'identité du responsable de traitement et donc « d'attribuer les responsabilités »[755] d'un tel traitement.

Concernant, d'abord, les critères relatifs à l'identité – personne physique ou morale, autorité publique, service ou tout autre organisme – le G29 considère que l'aspect personnel nécessite de se tourner en priorité vers la personne morale pour qui le traitement de données est réalisé. L'individu, personne physique, qui a mis en œuvre le traitement ne sera considéré comme responsable de traitement que s'il a agi « en dehors du cadre et de l'éventuel contrôle des activités de la personne morale »[756]. Concernant ensuite l'aspect fonctionnel de la définition – entendu comme celui permettant de savoir qui détermine la finalité et les moyens du traitement – le G29 distingue trois cas de figure. D'abord, la désignation du responsable de traitement peut résulter d'une compétence expressément prévue par un texte. Ensuite, celle-ci peut avoir lieu en vertu d'une désignation implicite découlant de règles juridiques générales. Enfin, ces deux cas de figure peuvent-être écartés au profit d'une « analyse des éléments factuels ou des circonstances de l'espèce »[757]. L'appréciation *in concreto* des éléments proposés est ainsi utilisée afin de déterminer *in fine* qui exerce précisément une influence de fait sur la détermination des moyens et de la finalité du traitement[758].

384. L'appréciation *in concreto*. Les deux premières catégories permettent, en principe, « de désigner l'organisme qui détermine avec davantage de fiabilité et

[755] G29, *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »*, adopté le 16 février 2010, WP 169, p. 4.
[756] *Ibid.*, p. 17.
[757] *Ibid*, p. 9.

peuvent facilement couvrir plus de 80 % des situations dans la pratique »[759]. Mais le recours à l'appréciation *in concreto* s'avère particulièrement utile, en droit des sociétés par exemple, pour déterminer qui de la filiale ou de la maison mère agit en tant que responsable du traitement. Cette situation est susceptible de se présenter en matière de *quantified-self* lorsque deux entités distinctes mais liées interviennent à différents moments de la collecte de données personnelles. Faisant suite à un avertissement de la CNIL à une société[760], le Conseil d'Etat a eu l'occasion de se prononcer sur ce point particulier en considérant que la qualification de responsable du traitement, appréciée *in concreto*, doit permettre d'apprécier quelle est la structure ayant décidé des éléments principaux de la collecte[761]. Le Conseil d'Etat, a relevé, pour déterminer l'identité du responsable de traitement, que la société en question décidait de la nature des données collectées, déterminait les droits d'accès à ces données ou encore, fixait leur durée de conservation.

Les éléments retenus par le Conseil d'Etat sont à mettre en lien avec le dernier critère d'identification du responsable de traitement proposé par le G29 et repris par le RGPD, le responsable de traitement étant celui qui « détermine les finalités et les moyens du traitement de données à caractère personnel »[762]. Il est donc nécessaire, selon les termes du G29, d'observer le degré de précision avec lequel « une personne doit déterminer les finalités et les moyens afin d'être considérée comme un responsable du traitement »[763]. A ce titre, la notion de « moyens » se veut large et concerne non seulement les moyens techniques mais également des questions plus larges telles que celles relatives à la nature des données traitées au moment de leur collecte. Concernant ensuite la détermination de la finalité, le responsable de traitement est celui qui en décide normalement la portée.

---

[758] *Ibid*, p. 12.
[759] *Ibid*, p. 13.
[760] CNIL, Délibération de la formation restreinte n°2011-205 du 6 octobre 2011 portant avertissement à l'encontre de la société X.
[761] CE, 12 mars 2014, n°354629.
[762] Cette solution est également retenue par la jurisprudence interne. Sur ce point, voir : TGI Montpellier, ord. réf., 28 octobre 2010, *Marie C. c/Google France et Inc*. ou encore, T. com. Paris, 1ère ch., 28 janvier 2014, *M. X. c/Google Inc. et Google France*.
[763] G29, avis n°1/2010, *op. cit*., p. 14.

La qualification de responsable de traitement n'est néanmoins pas exclusive et nécessite d'envisager les cas où plusieurs responsabilités peuvent être retenues.

2. Une qualification non-exclusive

385. Les dispositions de la loi Informatique et Libertés de 1978 se distinguaient, avant leur réforme, de celles de la directive de 1995. L'hypothèse d'une co-responsabilité de la détermination des finalités et des moyens du traitement n'était en effet pas évoquée en droit interne et celle-ci était également laissée de côté par la Convention 108 du Conseil de l'Europe. Unifiées par suite de l'adoption du RGPD, les définitions françaises et européennes de la notion de responsable de traitement mentionnent désormais directement le cas de la responsabilité conjointe. Celle-ci évoque, pour l'essentiel, des situations dans lesquelles on constate l'intervention de plusieurs acteurs dans le traitement de données à caractère personnel, ces différents acteurs intervenants en tant que responsables du traitement. Conformément à la définition précédemment évoquée, cette coresponsabilité repose sur une décision conjointe de la finalité du traitement et des moyens à mettre en œuvre pour l'effectuer.

Le G29 avait déjà eu l'occasion d'apporter des précisions sur la question de la co-responsabilité en invitant à vérifier, sous l'empire de la directive de 1995, si le responsable de traitement identifié agissait « seul ou conjointement avec d'autres ». Cette identification de la coresponsabilité s'appréciait, à l'image de la responsabilité dite unique, *in concreto*. Surtout, conformément à l'analyse retenue, cette coresponsabilité naissait lorsque plusieurs parties déterminaient, pour certaines opérations de traitement, « soit la finalité, soit les éléments essentiels des moyens qui caractérisent un responsable du traitement »[764]. Ainsi, une simple coopération ou un simple échange de données entre différentes entités n'était pas suffisante pour caractériser la coresponsabilité. En effet, seule la détermination commune d'éléments essentiels relatifs à la finalité ou encore aux moyens du traitement permettaient de retenir la coresponsabilité, celle-ci n'ayant pour autant pas vocation à être parfaitement égalitaire. Comme mentionné expressément par le G29, la participation

des parties à la détermination conjointe pouvait revêtir différentes formes, celle-ci n'étant pas nécessairement partagée de façon égale. Dans un cas, deux responsables de traitement pouvaient par exemple s'unir et déterminer ensemble les finalités et moyens d'une application de *running* permettant de procéder à la mesure du rythme cardiaque lors d'une course à pieds. Dans un autre cas, un responsable de traitement déterminait simplement la finalité – la mesure du rythme cardiaque – alors qu'un autre responsable déterminait simplement les moyens – recours à une application ou nature des données collectées pour réaliser la finalité.

386. Une solution harmonisée. L'adoption du RGPD a permis d'uniformiser la solution en matière de coresponsabilité d'un traitement de données personnelles. Insérée à l'article 26, la notion de responsabilité conjointe s'entend ainsi de la situation dans laquelle « deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement ». Dès lors, les responsables conjoints doivent désormais définir « de manière transparente leurs obligations respectives » et ce afin d'assurer le respect des exigences du règlement, notamment en matière des droits de la personne concernée et de mieux tenir compte de la diversité des situations susceptibles de se présenter[765]. Une telle solution doit permettre un meilleur encadrement des traitements de données réalisés et par ailleurs éviter que la responsabilité du traitement ne repose que sur une seule des entités ayant déterminé ses finalités et ses moyens.

L'intégration de la notion de responsabilité conjointe au sein du RGPD a permis d'harmoniser les solutions en la matière, étant donné la non-transposition de la notion par la LIL en 2004 et le recours, qui lui a été préféré, à la notion de sous-traitance. Une telle solution semblait pourtant contraire à l'esprit de la directive. Comme le révélait le regroupement des autorités de protection européennes, « la détermination du responsable du traitement devient une notion communautaire, qui revêt son propre sens indépendant dans le droit communautaire et ne varie pas au gré

[764] *Ibid*, p. 20.
[765] Sabine Marcellin, Jérôme Semik, « La responsabilité des traitements de données partagés dans un groupe », *Dalloz IP/IT*, 2017, p. 632.

des dispositions législatives nationales potentiellement divergentes »[766]. Jugée imprécise, cette notion de co-responsabilité qui a été supprimée au moment de la transposition[767], a pourtant survécu en droit interne grâce à la CNIL, cette dernière ayant eu l'occasion d'y faire référence dans sa doctrine mais également dans les autorisations[768] et dans les sanctions qu'elle prononçait. La CNIL a par exemple considéré que le réseau social Facebook ainsi que sa filiale irlandaise déterminaient conjointement les finalités d'un traitement – combinaison de données en vue de proposer de la publicité ciblée – et devaient donc être considérées comme conjointement responsables du traitement[769].

387. L'évolution possible de la qualification. La détermination précise du responsable de traitement est d'autant plus délicate qu'elle est susceptible de varier, comme le souligne notamment le sous-groupe *Quantified-Self* du groupe de travail « Données de santé » de l'AFCDP. En effet, en fonction du rôle confié à chacun des acteurs appelés à intervenir dans cet écosystème, une qualification juridique différente pourra être appliquée. Ainsi, « individu, fabricant, gestionnaire de compte, éditeur de services, hébergeur, éditeur de réseau social, développeur »[770], sont tous susceptibles de recevoir la qualification de responsable de traitement, dès lors qu'ils déterminent chacun pour leur compte les moyens et finalités du traitement conformément aux critères précédemment évoqués. Un fabricant d'objets connectés permettant de collecter des données sera responsable de traitement, tout comme un éditeur de services qui, sur la base de ces mêmes données, proposera des analyses complémentaires.

La responsabilité conjointe pourra être retenue dans certains cas, à condition que les finalités du traitement soient décidées de manière conjointe par les deux entités. Or, retenir une telle solution semble être source de sécurité juridique pour les

[766] G29, Avis n° 1/2010, 16 février 2010, WP 169, p. 12.
[767] Sénat, rapport n° 218, *op. cit.*, p.50.
[768] Voir notamment sur ce point : CNIL, délibération n° 2007-106 du 15 mai 2007 portant autorisation des applications informatiques nécessaires à la mise en œuvre de la phase expérimentale du dossier pharmaceutique ; CNIL, délibération n° 2008-008 du 22 janvier 2008 autorisant la mise en œuvre par la Ville de Paris et par la Société des Mobiliers Urbains pour la Publicité et l'Information d'un traitement de données à caractère personnel ayant pour finalité la gestion de fichiers de personnes à risques dans le cadre du système de location de vélos Vélib'.
[769] CNIL, délibération de la formation restreinte n° SAN 2017-006 du 27 avril 2017 prononçant une sanction pécuniaire à l'encontre des sociétés FACEBOOK INC. et FACEBOOK IRELAND.
[770] AFCDP, *Quantified-Self connecté et Informatique et Libertés*, *op. cit.*, p. 15.

individus. La multitude d'acteurs susceptibles d'intervenir dans le domaine du *quantified-self* rend l'identification du ou des responsables de traitement parfois complexe et retenir la responsabilité conjointe doit faciliter cette opération. Néanmoins, les critères mis en œuvre ne doivent pas occulter le cas de figure selon lequel une personne va agir pour le compte d'un responsable de traitement, notamment dans le cadre d'une opération de sous-traitance.

B. La qualification incidente de sous-traitant

388. Outre le cas précédemment évoqué d'une éventuelle responsabilité conjointe, le *quantified-self*, en raison des nombreux échanges de données entre différents acteurs, pose la question cruciale de la sous-traitance des opérations réalisées sur des données. Un certain nombre d'opérateurs ont en effet recours à des sous-traitants lorsqu'ils mettent en œuvre des traitements de données à caractère personnel et ce mécanisme est favorisé par l'utilisation d'objets connectés. Ayant principalement comme mission de transformer une activité en donnée informatique, ces objets nécessitent parfois le concours d'un tiers afin de pouvoir bénéficier d'une analyse des données relevées. Le régime de la sous-traitance, tel qu'il était entendu avant l'adoption du RGPD, s'est rapidement montré insuffisant dans l'encadrement des rôles des différents sous-traitants appelés à traiter des données. Bien qu'expressément mentionné par les textes qui soumettaient ceux-ci à des obligations distinctes de celles des responsables de traitement **(1)**, ce régime a cependant fait l'objet d'une nécessaire clarification **(2)**.

1. La soumission du sous-traitant à certaines obligations

389. La notion de sous-traitant de données personnelles ne faisait à l'origine – et à l'image de la notion de responsable de traitement – l'objet d'aucunes dispositions particulières. Qu'il s'agisse de la version initiale de la loi Informatique et Libertés ou bien de la Convention 108 du Conseil de l'Europe, aucun des deux textes ne faisait référence à ce statut. Ce n'est qu'avec la transposition de la directive de 1995 par la loi de 2004 que cette qualification fera l'objet d'une définition, le sous-traitant s'entendant alors de « toute personne traitant des données à caractère personnel pour

le compte du responsable de traitement »[771]. Alors que la directive faisait figurer la notion au sein du chapitre premier relatif aux définitions, tel n'était pas le cas de la loi Informatique et Libertés. Cette dernière ne reprenait en effet pas à son compte la liste des personnes susceptibles d'être qualifiées de sous-traitants. Surtout, au titre de la loi du 6 janvier 1978 modifiée en 2004, le sous-traitant n'avait pas d'obligations propres et ne pouvait donc, à ce titre, être directement tenu pour responsable.

390. Le respect d'instructions. Le mécanisme prévu à l'époque reposait de manière générale sur le respect, par le sous-traitant, des instructions qui lui étaient données par le responsable de traitement. Qu'il s'agisse de l'article 17 de la directive de 1995 ou de l'ancien article 35 de la loi, ces deux textes mentionnaient déjà que l'opération de sous-traitance devait être régie « par un contrat ou un acte juridique », ce dernier ayant notamment pour but de définir les obligations incombant au sous-traitant, que ce soit en matière de sécurité ou encore de confidentialité des données. La CNIL avait d'ailleurs eu l'occasion de rappeler qu'aux termes de l'article 35 de la loi et en matière de responsabilité, « la société qui recourt à un sous-traitant n'en demeure pas moins l'unique responsable du traitement »[772]. Ainsi, le sous-traitant ne pouvait être directement tenu pour responsable des manquements relatifs à a protection des données personnelles qui lui étaient reprochés, contrairement au responsable de traitement. Cependant, et conformément aux mécanismes du droit civil, ces derniers pouvaient en revanche engager la responsabilité contractuelle du sous-traitant.

391. Un mécanisme privilégié dans le cadre de l'automesure. Le mécanisme de la sous-traitance a particulièrement eu vocation à être mobilisé en matière de *quantified-self*. En effet et comme l'a révélé la doctrine, « les données transmises par le client à l'occasion du contrat, via un site Internet ou via une application, présentes sur un objet connecté, seront le plus souvent effectivement traitées par un tiers, distinct du contractant direct, en vue de la fourniture effective des services

[771] Article 35, Loi Informatique et Libertés modifiée en 2004.
[772] CNIL, délibération de la formation restreinte n°2013-091 du 11 avril 2013 prononçant un avertissement public à l'encontre de la société X.

contractuels au client »[773]. L'externalisation structurelle mise en œuvre par le *quantified-self* a donc favorisé le recours au mécanisme de la sous-traitance, en vue de la fourniture de services complémentaires aux individus. Un équipementier sportif souhaitant disposer d'une application permettant de mesurer l'activité physique pourra ainsi avoir recours à un sous-traitant qui procédera effectivement à l'analyse des données collectées. Les responsables de traitement ont ainsi progressivement confié la gestion de certains aspects du service à des tiers liés contractuellement. Ces derniers, n'ayant pas la charge de déterminer les finalités du traitement, mais simplement d'agir pour le compte du responsable de traitement, ont donc eu vocation à être qualifiés de sous-traitant.

A ce titre et conformément à l'ancien article 35 de la loi Informatique et Libertés, ces derniers devaient « présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34 ». Cet article imposait notamment de « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ». Aussi, le responsable de traitement était chargé de procéder aux vérifications des mesures de sécurité mises en œuvre par son sous-traitant et, en cas de préjudice, sa responsabilité était en tout état de cause engagée étant donné que c'était sur lui seul que pesait la responsabilité dudit traitement[774].

392. La responsabilité limitée du sous-traitant. Afin de favoriser la lisibilité des obligations pesant sur chacune des parties en présence, la CNIL avait développé des modèles de clauses de confidentialité à appliquer dans le domaine de la sous-traitance. Celles-ci avaient notamment pour objet de définir les conditions dans lesquelles le sous-traitant s'engageait à effectuer, pour le compte du responsable de traitement, les opérations de traitement de données à caractère personnel. Le sous-

[773] Juliette Sénéchal, « La fourniture de données personnelles par le client via Internet, un objet contractuel ? », *AJCA*, 2015, p.212.
[774] CNIL, délibération n°2014-298 de la formation restreinte du 7 août 2014 prononçant un avertissement à l'encontre de la société X.

traitant ne faisait donc l'objet, sous le régime de la loi Informatique et Libertés dans sa version antérieure, que d'une responsabilité limitée.

Pourtant, les développements de l'Internet des objets ont nécessité que celle-ci soit élargie afin de prendre au mieux en compte la pluralité d'acteurs intervenant dans un traitement de données. L'automesure connectée a permis de révéler l'étendue des opérations de sous-traitance et le RGPD a alors profondément renouvelé le spectre des obligations mises à la charge des sous-traitants.

2. La clarification du statut de sous-traitant

393. Un régime juridique précisé. La définition qui est donnée du sous-traitant est aujourd'hui similaire à celle qui était précédemment retenue, même si l'on constate le retour à une liste précise d'individus pouvant recevoir cette qualification : l'article 9 du RGPD définit le sous-traitant comme la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. Surtout, le sous-traitant fait maintenant l'objet d'un régime juridique précis qui est contenu à l'article 28 du RGPD. Ce dernier fait écho aux dispositions précédemment évoquées en rappelant les « garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées » qui doivent être mises en œuvre et ce afin que « le traitement réponde aux exigences du présent règlement et garantisse les droits de la personne concernée ». Cependant, la plus grande nouveauté instaurée par le Règlement est l'alignement du régime de responsabilité du sous-traitant sur celui du responsable de traitement[775]. Alors que celui-ci ne pouvait être précédemment tenu directement responsable, sauf cas de recours ultérieur de la part du responsable de traitement, le sous-traitant figure désormais aux côtés de celui-ci au titre des individus dont la responsabilité peut être engagée sur le fondement d'un manquement à la réglementation sur la protection des données personnelles[776].

[775] Gérard Haas, Amanda Dubarry, « Confidentialité et protection des données », *Dalloz IP/IT*, 2017, p. 322.
[776] A titre d'exemple, le considérant 13 du Règlement indique que son adoption est « nécessaire […] pour offrir aux personnes physiques de tous les Etats membres un même niveau de droits opposables et d'obligations et de responsabilités pour les responsables du traitement et les sous-traitants ». De même, le considérant 22 précise que « tout traitement de

Outre les obligations traditionnelles associées au statut de sous-traitant et contenues à l'article 32 du Règlement, celui-ci dispose désormais d'obligations nouvelles, calquées sur celles qui incombent au responsable de traitement. Celui-ci doit par exemple tenir « un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement »[777]. Il peut également être tenu de coopérer avec l'autorité de contrôle dans l'exécution de ses missions[778] ou encore de notifier au responsable de traitement toute violation de données à caractère personnel[779]. Surtout, le sous-traitant peut désormais être directement tenu pour responsable des manquements aux dispositions du règlement.

394. Une responsabilité juridique distincte. Comme le précise l'article 82 du texte, « toute personne ayant subi un dommage matériel ou moral du fait du violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi ». Le mécanisme de responsabilité mis en place ne repose donc plus exclusivement sur la faute du responsable du traitement : le sous-traitant peut désormais voir sa responsabilité retenue s'il ne parvient pas à démontrer que le dommage ne lui est pas imputable. Le fait qu'il puisse être sanctionné directement en lieu et place ou conjointement avec le responsable de traitement si les deux sont fautifs, est révélateur du champ d'application élargi des nouvelles règles de protection des données, celles-ci prenant mieux en compte les différents acteurs appelés à traiter des données.

395. Le rôle actif du sous-traitant. Le sous-traitant, outre les nouvelles règles relatives à sa responsabilité, se voit également confier un rôle nouveau, le rapprochant encore plus du responsable de traitement. Un rôle actif lui est en effet confié dans la protection des données personnelles et celui-ci se traduit notamment par la mise en œuvre de ce qui a pu être perçu comme « une obligation générale d'assistance et de coopération »[780]. L'article 28, 3, e) indique ainsi que le sous-

---

données à caractère personnel qui a lieu dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union devrait être effectué conformément au présent règlement ».
[777] Article 30, 2 du Règlement (UE) 2016/679.
[778] Article 31 du Règlement (UE) 2016/679.
[779] Article 33, 2 du Règlement (UE) 2016/679.
[780] Aurélie Banck, « GDPR et sous-traitance : un nouveau devoir de conseil ? », *Dalloz IP/IT*, 2017, p. 36.

traitant « aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III ». Par ailleurs et toujours au même article, il est indiqué que le sous-traitant « aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ». S'apparentant plus à une obligation de moyens que de résultat, le sous-traitant est ainsi tenu d'aider le responsable du traitement à assurer la sécurité de ce dernier ou à notifier les violations de données à caractère personnel à l'autorité de contrôle et aux personnes concernées.

396. La consécration d'une chaîne de sous-traitance. La LIL traitait auparavant simplement des personnes « agissant sous l'autorité du responsable de traitement ou de celle du sous-traitant »[781]. Le RGPD a donc permis, outre une refonte des obligations du sous-traitant, la clarification d'une situation qui n'était jusque-là pas explicitement mentionnée par la réglementation. La notion de chaîne de sous-traitants est en effet désormais explicitement consacrée par le règlement et celui-ci évoque, notamment dans son article 28, la possibilité pour le sous-traitant de recruter un autre sous-traitant « pour mener des activités de traitement spécifiques pour le compte du responsable du traitement ». Le sous-traitant, pour y procéder, doit obtenir « l'autorisation écrite préalable, spécifique ou générale du responsable du traitement ». Quant aux obligations qui incombent au second sous-traitant, celles-ci sont similaires à « celles fixées dans le contrat ou un autre acte juridique entre le responsable du traitement et le sous-traitant ». Le mécanisme de responsabilité repose dans ce cas sur le sous-traitant initial qui « demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations ». La solution retenue par le nouveau Règlement diffère donc de celle précédemment retenue en ce que le responsable de traitement n'est plus responsable des activités confiées par le premier sous-traitant au second, alors qu'il devait auparavant en endosser la charge.

[781] Article 35, Loi Informatique et Libertés modifiée en 2004.

Les mécanismes de collecte et d'analyse de données dans le cadre du *quantified-self* vont pleinement bénéficier de ce régime de responsabilité renouvelé. Les différents opérateurs susceptibles d'être mobilisés dans le cadre de l'automesure connectée – fabricants d'objets connectés dotés d'outils de mesure, développeurs, éditeurs de logiciels, hébergeurs – sont tous susceptibles d'intervenir dans le cadre d'une chaîne de sous-traitance. L'actualisation du cadre juridique applicable et la clarification des différents régimes de responsabilité permet ainsi de réduire considérablement les risques d'une éventuelle perte de maîtrise sur le traitement de données personnelles mis en œuvre.

Le constructeur d'un objet connecté chargé de collecter les données pourra avoir recours à un sous-traitant pour les analyser, qui lui-même pourra avoir recours à un second sous-traitant pour les stocker. Par exemple, le fabricant d'un bracelet connecté permettant de mesurer le rythme cardiaque, ne disposant pas forcément des compétences techniques pour proposer ce service, pourra avoir recours à l'expertise d'une autre entreprise qui, elle-même, décidera de faire stocker les données chez une entreprise spécialisée dans le *cloud*. Le responsable de traitement initial, constructeur de l'objet connecté, devra faire appel à un sous-traitant présentant « des garanties suffisantes » au sens du règlement et avec lequel il va conclure un contrat. Le sous-traitant devra obtenir l'accord préalable du responsable de traitement avant de recruter le second sous-traitant, ce dernier étant tenu « aux mêmes obligations en matière de protection de données que celles fixées dans le contrat ou un autre acte juridique entre le responsable du traitement et le sous-traitant ». Alors que la responsabilité du traitement incombera au premier responsable du traitement initial et au premier-sous-traitant, ce dernier sera également responsable des agissements du second sous-traitant. Ainsi, les récentes évolutions de la réglementation prennent en compte la gestion de plus en plus externalisée du traitement tout en renforçant la sécurisation des échanges.

§2. Une externalisation sécurisée

397. La réglementation relative à la protection des données personnelles a tendance à prendre en compte de manière progressive l'externalisation croissante des

traitements de données. L'identification des différents acteurs se fait de plus en plus précise et les mécanismes de mise en œuvre de la responsabilité sont ainsi facilités. Cette externalisation, en plus de l'identification des différents acteurs susceptibles d'intervenir, implique également un transfert constant d'informations, généralement nominatives. A ce titre, ce transfert entre différents acteurs identifiés nécessite d'être hautement sécurisé afin de garantir la protection des données personnelles des individus. Cette obligation de sécuriser les échanges en amont **(A)** est complétée, en aval, par la nécessité de limiter l'accès de ces données à des tiers **(B)**.

A. L'obligation de sécuriser les échanges

398. La structure du *quantified-self* repose, grâce à l'avènement des nouvelles technologies, sur un transfert constant d'informations entre plusieurs intervenants et plusieurs supports connectés. Cet échange constant de données nominatives, dans le cadre de l'automesure connectée, suppose cependant la mise en œuvre de garanties relatives à la sécurité, aussi bien techniques que juridiques. Cette obligation de sécurisation des échanges entre différents supports et différents opérateurs est rendue nécessaire par le fait que les objets utilisés dans le cadre de l'automesure connectée ont une capacité de stockage interne limitée, qui justifie donc que les données transférées fassent l'objet d'une protection lors de leur transit. Dès lors, bien que l'on assiste à un renouvellement du risque informatique par l'utilisation de ces nouvelles technologies **(1)**, la réglementation semble être à même de maîtriser ce risque **(2)**.

1. Le risque informatique accru

399. Le *quantified-self*, en reposant sur l'utilisation d'outils dotés de capteurs et de puces RFID permettant de collecter et de transmettre des informations sous forme de données, soumet l'individu à des risques de nature informatique, susceptibles de porter atteinte à ses données personnelles. Les dispositifs de *quantified-self*, tels que les bracelets connectés, ont en effet une interface limitée qui nécessite qu'ils soient reliés à un ordinateur plus performant afin d'analyser les données qu'ils auront collecté.

Le modèle de fonctionnement communément retenu repose ainsi sur une relation tripartite entre *tracker* d'activité, application mobile et dans certains cas, *cloud computing*[782]. La transmission entre chacun de ces dispositifs présente donc un risque pour les données personnelles et ces risques relatifs à la sécurité des données sont susceptibles de se manifester à chacune des étapes de la chaîne, entre collecte, transmission et stockage des données collectées.

400. La diversification des attaques informatiques. Les attaques informatiques se limitaient auparavant principalement au *phishing*[783] ou hameçonnage, technique visant à obtenir des informations concernant les individus en usurpant l'identité d'un tiers de confiance tel qu'une banque ou une administration. Celles-ci ont pourtant eu tendance à se développer et à se diversifier en même temps que les technologies numériques. A l'heure actuelle, ce sont par exemple les attaques par déni de service ou *DoS attack*, visant à saturer un réseau pour empêcher son utilisation, qui sont les plus répandues. Souffrant généralement d'un manque de sécurisation, les objets connectés sont aussi susceptibles de confronter leurs utilisateurs au vol, perte ou détournement des données qu'ils collectent[784]. De plus, l'informatisation des processus d'automesure révèle la double nature des atteintes auxquelles les individus risquent d'être confrontés. La cybercriminalité se manifeste dès lors « non seulement par des infractions strictement informatiques, comme les piratages et les cyberattaques des systèmes informatiques, mais aussi par des escroqueries, vols de données, abus de confiance, où l'informatique facilite le passage à l'acte dans la commission d'infractions classiques »[785]. Or, les objets connectés utilisés dans le cadre du *quantified-self*, par leur structure, présentent des garanties de sécurité moins efficaces que celles, par exemple, des ordinateurs. Le déploiement d'attaques informations s'en trouve facilité[786] et les failles de sécurité susceptibles de

[782] Mario Ballano Barcena, Candid Wueest, Hon Lau, « How safe is your quantified-self », *Security Response*, Symantec, 2014, p. 13
[783] Pour plus de précisions sur la notion, voir notamment : David Père, David Forest, « L'arsenal répressif du phishing », *Recueil Dalloz*, 2006, p. 2666.
[784] Bruno Sido, Anne-Yvonne Le Dain, *Sécurité numérique et risques : enjeux et chances pour les entreprises*, Rapport fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, n° 271, tome I (2014-2015) - 2 février 2015, p. 213.
[785] Myriam Quéméner, « Le rôle préventif de la justice en matière de cybersécurité », *Dalloz IP/IT*, 2016, p. 12.
[786] Demetrius Klitou, *Privacy Invading Technologies and Privacy by Design, Safeguarding Privacy, Liberty and security in the 21st century, Information Technology and Law Series*, Springer, 2014, p. 173.

toucher les données à caractère personnel sont multipliées par l'interconnexion de ces objets[787].

401. Trois types de risques. La *Federal Trade Commission* met l'accent, Outre-Atlantique, sur trois types de risques qui sont inhérents aux objets connectés[788]. Ceux-ci permettent en effet d'accéder plus facilement aux données personnelles, de rendre les autres systèmes encore plus vulnérables ou bien de présenter en eux-mêmes des failles de sécurité. Ces risques ne sont pas propres aux objets connectés mais leur nature, telle qu'évoquée précédemment, permet d'accentuer ces risques. Ainsi, l'Internet des Objets, pris dans sa globalité, semble offrir « une surface d'attaque considérable » en ne présentant pas « d'un point de vue architectural, de plateforme unifiée »[789]. Les entreprises commercialisant des objets connectés n'ont pas forcément la même expertise dans le domaine de la sécurité que les entreprises proposant des systèmes d'exploitation plus traditionnels[790]. De même, les objets connectés, notamment ceux entrant dans la catégorie des *trackers* d'activité physique, sont parfois le fruit du travail de jeunes startups ne possédant pas toujours les compétences propres à sécuriser l'objet qu'elle propose. La rencontre entre innovateurs dans le cadre d'incubateurs, tels que la Cité de l'objet connecté à Angers[791] ou l'IOT Valley à Labège[792], permet parfois de pallier ce type de problèmes en favorisant le partage du savoir et en sensibilisant les innovateurs aux problématiques juridiques.

2. L'identification juridique du risque

402. Les risques présentés peuvent être le fait de négligences de la part du responsable de traitement ou le résultat d'attaques informatiques[793]. Aussi, les différents textes relatifs à la protection des données ont-ils prévu la mise en œuvre de mesures visant à prévenir l'éventualité d'une atteinte aux données personnelles d'un

[787] Emmanuel Daoud, Géraldine Péronne, « Cyberattaques : la lutte s'intensifie », *AJ pénal*, 2015, p. 396.
[788] FTC, *Internet of Things : Privacy & Security in a Connected World*, 9 janvier 2015.
[789] Emmanuel Daoud, Flora Plénacoste, « Cybersécurité et Objets Connectés », *Dalloz IP/IT*, 2016, p. 409.
[790] Privacy Rights Clearinghouse, *Mobile Health and Fitness apps : what are the Privacy Risks*, posted July 2013, Revised December 2014.
[791] https://citedelobjetconnecte.com/
[792] https://www.iot-valley.fr/

individu[794]. La Convention 108 du Conseil de l'Europe adoptée en 1981 indiquait déjà dans son article 7 que « des mesures de sécurité appropriées sont prises pour la protection des données à caractère personnel enregistrées dans des fichiers automatisés contre la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisés ». La directive de 1995 traitait également de la sécurité des traitements et indiquait notamment que devaient être adoptées des « mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés », notamment lorsque ce traitement comportait « des transmissions de données dans un réseau »[795].

L'article 121 de la LIL réécrite dispose de façon simplifiée que le responsable de traitement est tenu de « « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ». Le Code pénal, dans un article 226-17, précise les sanctions applicables lorsqu'un traitement est réalisé sans que les mesures permettant d'assurer la sécurité des données collectées soient mises en œuvre, celles-ci pouvant atteindre cinq ans d'emprisonnement et 300 000 euros d'amende.

403. L'absence de précision sur les mesures à mettre en œuvre. Malgré les diverses dispositions relatives à la sécurité contenues dans l'ensemble de la réglementation, aucune précision n'a véritablement été apportée quant aux précautions utiles ou autres mesures techniques que le responsable de traitement doit mettre en œuvre afin de sécuriser le traitement de données à caractère personnel. La directive de 1995 indiquait tout au plus que le niveau de sécurité devait être fonction de l'état de l'art et des coûts liés à leur mise en œuvre, introduisant ainsi un principe de proportionnalité. S'apparentant à une obligation de moyen renforcée, l'obligation

[793] Jacques Francillon, « Cyberdélinquance. Piratage informatique. Maintien frauduleux dans un STAD. Vol de données », *RSC*, 2015, p. 887.
[794] Gérard Haas, « La cybercriminalité à la fois côté obscur et face cachée du Big Data », *Dalloz IP/IT*, 2016, p. 21.
[795] Article 17 de la Directive 95/46/CE.

de sécurité était évaluée par la CNIL en fonction de l'efficacité des mesures mises en œuvre par le responsable de traitement[796]. Dès 1981, l'autorité administrative s'était prononcée sur l'étendue de ces mesures de sécurité, en estimant que celles-ci devaient porter sur la fiabilité des matériels et des logiciels[797].

Plus récemment, la CNIL a eu l'occasion de prononcer un avertissement à l'encontre d'une société proposant un régime alimentaire personnalisé en raison du manque de sécurisation des échanges, au regard de la sensibilité des données collectées[798]. En l'espèce, une société proposait à des internautes de s'inscrire, via son site Internet, à un programme alimentaire personnalisé. La CNIL a relevé que les mots de passe des clients et prospects ainsi que certaines données personnelles étaient conservées sans sécurisation. La solution retenue se révèle particulièrement intéressante pour le domaine de l'automesure connectée puisque les éléments relevés – historique de poids, habitudes alimentaires, pratique sportive, consommation d'alcool – font partie des catégories de données classiquement recueillies dans ce cadre. Celle-ci a donc permis de rappeler la nécessité de sécuriser les échanges, notamment par le chiffrement, lorsque de telles données font l'objet d'un traitement. Cette décision est à rapprocher du fait que la responsabilité du responsable de traitement peut être recherchée lorsqu'il est lui-même à l'origine d'une divulgation fautive à un tiers non-autorisé, conformément à l'article 226-22 du Code pénal qui sanctionne le fait de communiquer à des tiers non autorisés des données à caractère personnel, « dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ».

404. Le cas particulier des données sensibles. Les données personnelles sensibles font, du moins pour certaines d'entre elles, l'objet de dispositions complémentaires visant à garantir leur sécurité. L'article 68 de la LIL indique par exemple, concernant les données soumises au secret professionnel, que leur transmission doit être effectuée dans des conditions de nature à garantir leur

[796] CNIL, Délibération de la formation restreinte n°2012-176 du 21 juin 2012 portant avertissement à l'encontre de la Société Européenne de Traitement de l'Information (Groupe Crédit Mutuel).
[797] CNIL, Délibération 81-94 du 21 juillet 1981 portant adoption d'une recommandation relative aux mesures générales de sécurité des systèmes informatiques.
[798] Délibération de la formation restreinte n°2014-261 du 26 juin 2014 prononçant un avertissement rendu public à l'encontre de la société Régime Coach.

confidentialité, étant entendu que la CNIL peut « adopter des recommandations ou des référentiels sur les procédés techniques à mettre en œuvre ». Au regard de l'évolution rapide des technologies de l'information et des menaces informatiques, l'éventail des mesures de sécurité disponibles fait surtout l'objet de développements au sein de documents indépendants des textes législatifs. Mis au point par différents organismes, ces référentiels de sécurité ont permis de présenter les mesures techniques à adopter pour sécuriser les traitements de données personnelles. Dès 2014 par exemple, la CNIL a adopté un label en matière de services de coffre-fort numérique[799]. Plus largement, celle-ci publie régulièrement des guides contenant des recommandations à mettre en œuvre[800]. Mis à jour, ceux-ci présentent notamment les mesures minimales de sécurité à mettre en œuvre, qu'il s'agisse des mesures de sécurité relatives à l'informatique mobile ou encore aux serveurs[801].

405. Par ailleurs, l'obligation de sécurité précisée par la loi Informatique et Libertés peut également être appréciée au regard de recommandations qui sont fournies par d'autres institutions. A ce titre, l'Agence nationale pour la sécurité des systèmes d'informations (ANSSI) a eu l'occasion d'apporter certaines autres recommandations relatives par exemple à la sécurisation des sites web[802] ou des smartphones[803]. Celle-ci recommande par exemple d'interdire l'accès au service de géolocalisation pour les applications qui n'utilisent pas cette fonction ou encore de chiffrer les échanges d'informations sensibles[804]. Ces documents permettent d'identifier précisément les risques techniques encourus[805], risques qui sont par ailleurs limités par une obligation de minimisation des échanges de données.

B. L'obligation de minimiser les échanges

406. La réglementation dédiée à la protection des données personnelles cherche, dans son ensemble, à établir un juste équilibre entre la possibilité de mettre

[799] CNIL, Délibérationn°2014-017 de la CNIL du 23 janvier 2014 portant adoption d'un référentiel pour la délivrance de labels en matière de coffre-fort numérique.
[800] CNIL, *Guide sur la sécurité des données personnelles*, 2010, 30 p.
[801] CNIL, *Guide sur* la *sécurité des données personnelles*, 2017, 32 p.
[802] ANSSI, *Recommandations pour la sécurisation des sites web*, 13 août 2013, 23 p.
[803] ANSSI, *Recommandations de sécurité relatives aux ordiphones*, 28 juillet 2015, 10 p.
[804] *Ibid*, p. 7.
[805] Cf., *supra*, n° 400.

en œuvre des traitements de données personnelles et la nécessité de protéger les droits et libertés des citoyens[806]. A ce titre, les règles en vigueur reposent sur la nécessité d'empêcher que des tiers puissent avoir accès, sans autorisation, à des données personnelles. La réglementation impose dès lors d'identifier avec précision les acteurs concernés et de superviser les traitements qui sont mis en œuvre. Il est donc nécessaire, pour déterminer l'étendue du droit d'accès aux données, d'identifier précisément la personne concernée par le traitement de données personnelles **(1)**, les modalités de supervision du traitement pouvant, elles, être réalisées par une personne extérieure à celui-ci **(2)**.

1. La notion de personne concernée par le traitement

407. L'enjeu de l'accès aux données. L'accès aux données personnelles est subordonné, en vertu de la loi Informatique et Libertés, à l'identification de la personne concernée par le traitement. Avant sa réécriture, la loi en donnait une définition précise dans son article 2 en considérant qu'il s'agit de « celle à laquelle se rapportent les données qui font l'objet du traitement ». Cette définition explicite a disparu du texte par suite de sa réécriture et c'est donc au RGPD qu'il faut désormais se référer. Celui-ci ne donne pas de définition précise mais il est indiqué à l'article 4, 1° que la « personne concernée » est une personne physique identifiée ou identifiable à laquelle se rapporte toute information. Ainsi, alors que la notion de responsable de traitement ou de sous-traitant permet de définir quelles sont les obligations associées à la mise en œuvre d'un traitement de données, l'identification de la personne concernée par le traitement permet de déterminer le titulaire des droits garantis par la réglementation quant à la protection des données personnelles, au titre desquelles figure notamment le droit d'accès.

La notion de personne concernée, déjà exprimée par la Convention 108 du Conseil de l'Europe, vise ainsi à exprimer « l'idée selon laquelle toute personne possède un droit subjectif par rapport aux informations qui la concernent, même si

[806] Emmanuel Derieux, « Vie privée et données personnelles – Droit à la protection et « droit à l'oubli » face à la liberté d'expression », *Les Nouveaux Cahiers du Conseil constitutionnel*, 2015/3, n°48, p. 21 à 33.

ces informations sont rassemblées par d'autres »[807]. En tout état de cause, il est permis d'hésiter lorsque la personne concernée par un tel traitement décède. Comme la doctrine a pu le souligner, « des informations sur les personnes décédées peuvent concerner des personnes vivantes, comme par exemple une maladie héréditaire »[808]. Une telle situation est justement susceptible de se produire dans le cadre du *quantified-self*. Des objets connectés capables de mesurer le taux de glucose d'une personne diabétique sont désormais disponibles et cela pose la question de savoir si les ayants-droits de la personne concernée peuvent avoir accès aux informations collectées.

La loi Informatique et Libertés ne prévoyait à l'origine que la possibilité pour les héritiers de la personne concernée par un traitement de données personnelles de faire actualiser les données la concernant[809]. Le Conseil d'Etat, en confirmant une délibération de la CNIL en date du 29 mai 2013[810], a d'ailleurs eu l'occasion d'indiquer qu'en vertu des articles 2 et 39 de la loi Informatique et Libertés, seule la personne à laquelle se rapportent des données à caractère personnel peut obtenir communication de ces données. Par conséquent, la plus haute juridiction administrative a indiqué que les ayants droit ne sont pas des personnes concernées au sens du texte[811]. Pour reprendre l'exemple du dispositif de *quantified-self* permettant de mesurer le taux de glucose, les ayants-droits de la personne concernée ne seraient pas en mesure d'accéder aux données, même s'ils ont un intérêt à le faire. Cette situation, susceptible de limiter certains bénéfices du *quantified-self*, a cependant fait l'objet d'un encadrement spécifique avec l'adoption de la loi pour une République numérique.

408. Le cas particulier de la mort numérique. La loi pour une République numérique n'a pas eu vocation à modifier les critères relatifs à l'identification de la

[807] Rapport explicatif de la Convention STE n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, p. 29.
[808] Anne Debet, Jean Massot, Nathalie Metallinos, *Informatique et Libertés, La protection des données à caractère personnel en droit français et européen*, *op. cit.*, p. 285.
[809] L'article 40 de la loi de 1978, dans sa version en vigueur jusqu'au 9 octobre 2016, indiquait ainsi : « Les héritiers d'une personne décédée justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence. ».
[810] Conseil d'État, Section du contentieux, 10ème et 9ème chambres réunies, n° 386525, 8 juin 2016.
[811] Jean-Marc Pastor, « Des données personnelles ne peuvent pas être transmises aux ayants droit », *Dalloz actualité*, 20 juin 2016.

personne concernée. Cependant, elle a permis de préciser les contours d'un nouveau droit, relatif à la mort numérique[812]. En insérant un article 40-1 au sein de la loi de 1978, devenu l'article 85 après la réécriture, le texte a eu pour effet de préciser les modalités selon lesquelles une personne peut, de son vivant, organiser les conditions de conservation, d'effacement et de communication de ses données à caractère personnel après son décès[813]. Bien que les droits sur les données personnelles s'éteignent toujours au décès de leur titulaire, leur maintien est prévu pour le cas où l'individu a préparé des directives en ce sens – générales lorsqu'elles concernent l'ensemble des traitements de données concernant l'individu ou particulières lorsqu'elles n'en concernent que certains – ou lorsque ce maintien se fait, dans certains cas précis, au bénéfice des héritiers. Cette disposition présente un intérêt particulier pour l'automesure, une personne utilisant un dispositif de *quantified-self* pouvant désormais prévoir, de son vivant, que ses héritiers auront accès aux données relevées. Ces derniers peuvent en effet bénéficier de l'accès à certaines informations, qu'il s'agisse du taux de glucose de la personne diabétique, mais aussi de certaines intolérances alimentaires, allergies ou maladies héréditaires. Par exemple, un individu atteint de la maladie de Huntington, affection neurodégénérative du système nerveux, pourrait porter un bracelet connecté mesurant l'intensité de la foulée pour déceler l'avancée de la maladie et son effet sur la motricité. Les héritiers de cette personne auront un intérêt particulier à avoir accès à de telles informations, étant donné le caractère héréditaire de cette maladie[814].

Ces dispositions relatives à la mort numérique n'ont pas été reprises par le RGPD. Celui-ci précise simplement les critères d'identification applicables à la personne concernée par le traitement.

409. Les critères d'identification renforcés par le RGPD. Le RGPD se prononce en faveur d'un renforcement des garanties à apporter quant à l'identification de la personne concernée en indiquant que « le responsable du traitement devrait prendre toutes les mesures raisonnables pour vérifier l'identité d'une personne

[812] Cécile Pérès, « Les données à caractère personnel et la mort, Observations relatives au projet de loi pour une République numérique », *Recueil Dalloz*, 2016, p. 90.
[813] Article 63 de la loi n°2016-1321 du 7 octobre 2016.
[814] https://www.inserm.fr/information-en-sante/dossiers-information/huntington-maladie

concernée qui demande l'accès à des données, en particulier dans le cadre des services et identifiants en ligne ». Une telle disposition, bien que non intégrée directement dans le corps du Règlement, est cependant susceptible de trouver un écho pratique, pour le cas ou deux ou plusieurs personnes utilisent potentiellement le même dispositif de *quantified-self*. Des membres d'une même famille pourraient ainsi se partager un même bracelet connecté lors de séances de sport. Une telle hypothèse pourrait rendre l'identification de la personne concernée par le traitement plus délicate et nécessiterait ainsi la mise en œuvre de vérifications renforcées de la part du responsable de traitement. Surtout, le considérant 62 fait également écho aux modalités d'exercice du droit d'accès. Celles-ci, également précisées dans une délibération de la CNIL[815] ainsi que dans le décret d'application de la loi de 1978[816], précisent ainsi que « le responsable du traitement doit s'assurer de l'identité du demandeur, notamment par la production d'un titre d'identité ». De telles dispositions s'inscrivent notamment dans la continuité des modalités d'accès dont bénéficient les tiers et les destinataires d'un traitement de données.

2. Les notions de tiers autorisés et de destinataire

410. La loi Informatique et Libertés et le Règlement général européen reposent sur la mise en œuvre d'une protection des données personnelles des individus face aux risques éventuels d'accès par des tiers aux données traitées. Certaines catégories de personnes font pourtant exception à ce principe d'interdiction, qu'il s'agisse des tiers autorisés et des destinataires.

L'article 3 de la loi Informatique et Libertés précisait, dans sa rédaction initiale, la définition du destinataire en indiquant qu'il s'agissait de « toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données ». Cette définition élargie figure désormais au sein du RGPD. Celui-ci, dans son article 4, 9°, identifie ainsi le

[815] CNIL, Délibération n°80-10 du 01 avril 1980 portant adoption d'une recommandation relative à la mise en œuvre du droit individuel d'accès aux fichiers automatisés.
[816] Article 98 du décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

destinataire comme étant « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers ».

411. La définition du destinataire présente un intérêt pratique, puisqu'elle permet de définir à l'avance le spectre des individus ayant vocation à recevoir la communication des données collectées. En effet, les formalités préalables subsistantes à la mise en œuvre d'un traitement de données – qu'il s'agisse d'une déclaration ou d'une demande d'autorisation ou d'avis – doivent faire mention des « destinataires ou catégories de destinataires habilités à recevoir communication des données ». Surtout, la notion de destinataire est soumise à une appréciation *in concreto* entre données personnelles et finalité du traitement, en fonction des qualités nécessaires à son habilitation et qui lui permettent d'avoir accès aux données faisant l'objet d'un traitement[817]. Le Conseil d'Etat semble faire application de ces critères dans sa jurisprudence, comme le révèle un arrêt du 21 mars 2011. En l'espèce, le ministre de l'Intérieur, de l'outre-mer et des collectivités territoriales avait pris un arrêté procédant à la création d'un traitement automatisé ayant pour objet « la gestion des pièces administratives du droit de circuler des véhicules ». Le requérant contestait la légalité de cet arrêté car il ne mentionnait pas, parmi les destinataires des données traitées, les organismes chargés du contrôle technique automobile. Le Conseil d'Etat, recherchant d'abord les habilitations nécessaire pour procéder à la signature d'un tel acte, a vérifié les mentions relatives aux destinataires pour constater que les organismes chargés du contrôle technique automobile n'en faisaient pas partie[818].

412. L'accès par des tiers extérieurs au traitement. Une précision, reprise par le Règlement européen[819], doit cependant être apportée étant donné que « les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à demander au responsable du traitement de leur communiquer des données à caractère personnel ne constituent pas des destinataires ». Ainsi, outre les destinataires, il est possible de retenir la qualification

[817] Romain Perray, *JurisClasseur Administratif*, fascicule 274-10, p. 54.
[818] Conseil d'Etat, 21 mars 2011, n° 329879, *Syndicat national du contrôle technique automobile*.

de tiers autorisés, entendue au sens de la loi Informatique et Libertés comme regroupant « les personnes habilitées par des textes législatifs ou réglementaires à obtenir un accès ponctuel et limité aux données »[820]. Plusieurs cas de figure sont proposés par la CNIL. Cette dernière présente ainsi, parmi les tiers autorisés, les autorités judiciaires, les experts ou enfin les agents de l'administration fiscale. Les médecins ou pharmaciens – qui pourraient vocation à obtenir des données issues de dispositifs d'automesure connectée – ne sont donc pas, en théorie, considérés comme des tiers autorités au sens de la réglementation. Mais ceux-ci peuvent être mentionnés parmi les destinataires du traitement, à condition que la personne concernée en soit informée, conformément à l'article 13 du RGPD.

La notion de tiers autorisé permet surtout de justifier l'accès à des données personnelles par des tiers extérieurs au traitement, par exemple pour les besoins d'une enquête. L'article 77-1-1 du Code de procédure pénale dispose à ce titre que « le procureur de la République ou, sur autorisation de celui-ci, l'officier de police judiciaire, peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des informations intéressant l'enquête, y compris celles issues d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces informations, notamment sous forme numérique, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel ».

413. L'accès à un nombre important d'informations. La possibilité pour des enquêteurs d'avoir accès aux données issues d'objets connectés augmente considérablement le spectre d'informations auxquelles ils sont susceptibles d'avoir accès. Les objets connectés, notamment ceux d'automesure, ont cette particularité de permettre une multiplication des sources de données et de définir avec précision un certain nombre de mesures de nature diverse. Qu'il s'agisse d'informations relatives à la géolocalisation combinées par exemple avec les données horaires, il est ainsi

[819] Sur ce point, l'article 4, 9° du Règlement indique que « les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ».
[820] CNIL, *Guide Professionnels de santé*, 2011, p. 9.

possible de déterminer avec une certaine précision les déplacements d'un individu. Une telle hypothèse s'est d'ailleurs récemment produite dans le cadre d'une enquête aux Etats-Unis, les policiers ayant eu accès aux données d'un bracelet connecté, *tracker* d'activité physique, afin d'avoir accès à de nouvelles informations[821]. En l'espèce, un homme avait indiqué aux enquêteurs qu'un individu s'était introduit chez eux à une certaine heure pour tuer sa femme. Les informations relevées grâce au *tracker* ont permis de montrer que le décès avait eu lieu bien plus tard, invalidant ainsi l'alibi du mari, qui s'est finalement révélé être l'assassin.

La pratique du *quantified-self* repose sur le recours à de nombreux opérateurs susceptibles d'intervenir dans la chaîne du traitement des données. La réglementation a progressivement évolué pour prendre en compte ces différents acteurs et pour faciliter leur identification. Les modalités d'accès aux données des individus ont donc fait l'objet d'un encadrement précis et les possibilités de réutilisation des données personnelles ont également été amenées à faire l'objet de dispositions précises.

SECTION II. UNE RÉUTILISATION ENCADRÉE

414. L'enjeu des règles relatives à la protection des données personnelles est de pouvoir s'assurer, conformément à l'article premier de la loi de 1978, que le développement de l'informatique ne porte atteinte « ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». Ce principe général de protection se trouve pourtant confronté aujourd'hui à une amplification considérable des moyens de collecte des données.

415. Surtout, le flot d'informations disponibles et l'utilisation croissante d'objets connectés s'inscrivent aujourd'hui dans une logique de *big data*, entendue comme la faculté d'analyser des ensembles non-structurés de données provenant de sources variées[822]. Les capacités de croisement de données potentiellement identifiantes, notamment à des fins commerciales, sont donc susceptibles de présenter

[821] https://www.lesechos.fr/26/04/2017/lesechos.fr/0212015659980_quand-les-objets-connectes-aident-la-police-a-resoudre-des-affaires-criminelles.htm
[822] Alexandra Bensamoun, Célia Zolynski, « Cloud computing et big data. Quel encadrement pour ces nouveaux usages des données personnelles ? », *Réseaux*, 1/2015, n° 189, p. 103-121.

un risque pour les individus. Les termes de la loi Informatique et Libertés, bien que montrant parfois des limites face au développement des nouvelles technologies, ont dans certains cas fait preuve d'une grande capacité d'adaptation. Certains principes de protection, font aujourd'hui encore la preuve de leur pérennité **(Paragraphe 1)** et ils permettent d'encadrer efficacement les cas de réutilisation des données personnelles **(Paragraphe 2)**.

§1. L'actualisation des principes « Informatiques et Libertés »

416. La loi Informatique et Libertés entend donner à l'individu une certaine maîtrise sur l'utilisation qui peut être faite de ses données personnelles[823]. Pour y parvenir, elle exige que les traitements de données mis en œuvre respectent certains principes ayant pour but de limiter l'étendue de la collecte et d'encadrer les éventuelles utilisations ultérieures. Ceux-ci ont d'ailleurs été profondément renouvelés en raison du développement de nouveaux outils numériques. La définition désormais élargie de la notion de traitement de donnée à caractère personnel **(A)** a ainsi permis aux principes protecteurs d'être appliqués largement et donc de prendre en compte le parcours qui est réalisé par la donnée **(B)**.

A. La conception extensive de la notion de traitement de données

417. La réglementation Informatique et Libertés, afin de survivre à la rapidité des évolutions technologiques, a dû adopter un cadre large[824]. Cela s'est notamment traduit par l'adoption de définitions extensives et malléables, à l'image de la définition évolutive associée à la notion de donnée à caractère personnel. Cette approche extensive de la réglementation permet dès lors la prise en compte du *quantified-self* dans la mise en œuvre de règles protectrices pour l'individu. Qu'il s'agisse des termes employés par la réglementation Informatique et Libertés **(1)** ou des précisions jurisprudentielles qui ont été apportées par la suite **(2)**, l'automesure

[823] Sur ce point, l'article 1, alinéa 2 du texte, indique 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 ».
[824] Rapport du Conseil d'Etat, *Le Numérique et les droits fondamentaux*, op. cit., p. 86.

connectée semble en théorie aujourd'hui entrer dans la définition du traitement de données.

1. Une définition légale élargie

418. Alors que « l'accumulation de termes montre la volonté de donner un sens large au mot traitement »[825], la définition légale retenue par la loi Informatique et Libertés permet en effet de retenir une acception large de ce terme, le but étant de pouvoir y inclure la moindre opération effectuée sur des données personnelles. Le texte, modifié dès 2004 par la transposition de la directive de 1995, énumère en effet une liste non exhaustive d'opérations constitutives de traitements. Ainsi, « constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction » [826].

La loi du 6 août 2004 a ainsi apporté certaines modifications aux dispositions relatives au traitement, contenues dans le texte initial de la loi Informatique et Libertés. La définition donnée a ainsi intégré de nouveaux procédés liés aux développements technologiques, permettant d'élargir le spectre de l'opération de traitement[827]. Ont ainsi été pris en considération « la communication par transmission », la « consultation » et la « diffusion » de données à caractère personnel[828]. Par ailleurs, la référence au caractère automatisé du traitement a disparu afin d'inclure dans la notion de traitement, non seulement les traitements automatisés de données, mais également les traitements manuels à condition que ceux-ci soient intégrés à des fichiers.

---

[825] Jean Frayssinet, « La protection des données personnelles », in A. Lucas, J. Devèze et J. Frayssinet, *Droit de l'informatique et de l'internet*, PUF, 2001, n° 122.
[826] Article 2 al. 1er de la loi n° 78-17 telle que modifié par la loi n° 2004-801 du 6 août 2004.
[827] Jurisclasseur Administratif, *op. cit.*, p. 41.
[828] Sénat, Rapport n° 218, 19 mars 2003, *op. cit.*, p. 48.

419. Les précisions sur la notion de fichier. Le RGPD reprend en substance la même définition dans son article 4 relatif aux définitions. Certaines précisions sont cependant apportées concernant la notion de « fichier », l'ensemble structuré de données constitué par ce dernier pouvant ainsi être « centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique »[829]. Ainsi et alors que « nous ne pouvons que nous méfier chaque jour d'avantage du postulat fragile de l'impossibilité technologique de tel ou tel traitement »[830], adopter une définition large de cet acte permet à la réglementation d'être appliquée, peu importe l'outil ou le dispositif employé pour manipuler des données personnelles. En effet, « nombreux sont ceux qui soulignent la qualité de cette définition au caractère suffisamment souple et flexible, qui a permis à la directive de s'adapter sans mal aux évolutions technologiques »[831].

Parmi les évolutions technologiques en question, l'automesure connectée est sans doute celle qui bouscule le plus cette réglementation. L'explication, simple, réside dans le caractère multimodal de celle-ci et dans la diversité des dispositifs connectés ayant pour objet un échange automatique d'informations, objectif affirmé de l'Internet des objets[832]. Or, grâce à la miniaturisation et à l'accessibilité de ces nouveaux outils[833], les modalités de mise en œuvre d'un traitement de données sont démultipliées, justifiant ainsi l'acception large de la notion de traitement. La multiplication d'objets dotés de capteurs de nature différente entraîne en effet une augmentation du nombre de traitements réalisés. Les termes larges de la réglementation permettent donc de les prendre en compte, peu importe l'objet utilisé pour y procéder. Ainsi, le caractère large des définitions proposées par les textes a permis une intégration de nombreuses opérations. Mais leur formulation a posé certains problèmes d'interprétation auxquels la jurisprudence a dû apporter des réponses.

---

[829] Article 4 du Règlement (UE) 2016/679.
[830] Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *L'autodétermination informationnelle à l'ère de l'Internet*, Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications, Eléments de réflexion sur la Convention n°108 destinés au travail futur du Comité consultatif, Strasbourg, le 18 novembre 2004.
[831] Anne Debet, « Informatique et libertés : faut-il aujourd'hui réviser la directive 95/46/CE relative à la protection des données personnelles ? », *Recueil Dalloz*, 2011, p. 1034.
[832] Xiaofeng Lu, Zhaowei Qu, Qi Li, and Pan Hui, « Privacy Information Security Classification for Internet of Things Based on Internet Data », *International Journal of Distributed Sensor* Networks, 2015, vol. 2015.
[833] Daniel Kellmereit, Daniel Obodovski, *The Silent Intelligence, The Internet of Things*, DND Ventures LLC, 2013, 156 p.

2. Des précisions jurisprudentielles évolutives

420. Le cas des traitements réalisés manuellement. Le *quantified-self*, regroupant des pratiques ayant vocation à relever des données relatives au corps humain, repose sur la mise en œuvre de traitements qui sont généralement automatisés. Pourtant, il existe des cas dans lesquels les traitements ne sont pas exclusivement réalisés de cette manière : l'individu peut en effet relever manuellement des informations relatives à son activité. Un coureur souhaitant mesurer l'évolution de sa progression pourra par exemple consigner, dans un fichier Excel, les temps réalisés lors de ses différentes courses, relevés grâce à une montre classique. Un individu suivant un régime alimentaire pourra également noter manuellement la composition de ses repas et le nombre estimé de calories ingérées. Ces traitements, qui reposent sur une collecte de donnée réalisée sans dispositif connectée, font également partie des pratiques du *quantified-self* lorsque les résultats sont consignés dans un fichier informatique. Ils permettent donc de mobiliser la notion de « traitements non automatisés de données à caractère personnel contenues ou appelés à figurer dans des fichiers ».

Cette précision a engendré – par suite de son intégration à la réglementation par la loi du 6 aout 2004 en vue d'élargir le spectre de la notion de fichier[834] – certaines difficultés d'interprétation, comme l'a relevé la jurisprudence. Désormais incluse au sein de la définition du traitement, la notion de fichier apparaît comme étant l'élément permettant de mettre en œuvre la réglementation lorsque celle-ci concerne des opérations dites « non automatisées ». Ainsi, selon l'article 2 de la loi de 1978 modifiée et toujours en vigueur, les dispositions relatives aux traitements non automatisées ne s'applique que si les données sur lesquelles portent ces traitements sont « contenues ou appelés à figurer dans des fichiers ». Dès lors, ce n'est que dans le cas où un traitement est non automatisé qu'il faut se référer à la notion de fichier, élément sur lequel la jurisprudence a eu l'occasion d'exercer un contrôle.

421. Les critères de qualification : un fichier structuré et stable. Le Conseil d'Etat, se prononçant pour donner suite à une décision de sanction de la CNIL, avait

[834] Conseil de l'Europe, *Les nouvelles technologies : un défi pour la protection de la vie privée ?*, Strasbourg, 1989, p. 35.

eu l'occasion de montrer que les données à caractère personnel figurant dans des documents papiers du dossier individuel du salarié constituaient bien un fichier « au sens des dispositions précitées de l'article 2 de la loi du 6 janvier 1978 »[835]. La qualification retenue permettait dès lors de régulièrement appliquer les dispositions relatives à la loi Informatique et Libertés, en l'espèce, celles concernant le droit d'accès. Deux critères cumulatifs devaient cependant être identifiés afin de retenir cette qualification. En effet, et conformément au texte de la loi en vigueur jusqu'en novembre 2018, un fichier devait justifier de deux caractéristiques essentielles pour valablement prétendre recevoir cette qualification.

Comme le mentionnait l'ancien alinéa 4 de l'article 2 de la loi, ce fichier devait constituer un ensemble structuré et stable de données à caractère personnel. Le Conseil d'Etat, selon une jurisprudence constante, s'attachait à relever les critères relatifs à la structure et à la stabilité des données pour considérer que celles-ci puissent faire l'objet d'un « traitement non automatisé de données personnelles contenues ou appelées à figurer dans un fichier » [836]. En l'absence de ces deux caractères relatifs à la stabilité et à la structure, la qualification de fichier ne pouvait donc être retenue, entraînant dès lors l'exclusion des règles relatives à la protection des données personnelles. Selon cette interprétation, les informations relatives à un coureur relevant l'évolution de ses courses, consignées au crayon sur des feuilles volantes, ne présentaient pas les critères relatives à la structure et à la stabilité.

422. L'abandon du critère relatif à la stabilité. Les critères de qualification de la notion de fichier ont cependant été amenés à évoluer par suite de l'entrée en application du nouveau cadre européen de protection des données. Le RGPD a en effet procédé à l'abandon du critère relatif à la stabilité du fichier en mentionnant à l'article 4, 6° que celui-ci est constitué par « tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés » en précisant que cet ensemble peut être « centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ».

[835] Conseil d'Etat, 20 oct. 2010, n° 327916, *Sté Centrapel* : JurisData n° 2010-019120.
[836] Conseil d'Etat, 26 nov. 2010, n° 323694, *Monsieur A. et a.* : JurisData n° 2010-022087.

Une solution similaire doit être retenue en matière de *quantified-self* afin qu'un fichier soit protégé. Le fichier dans lequel seront retranscrites les données collectées de façon non-automatisée devra présenter ce critère relatif à la structure afin que les règles protectrices du RGPD et de la loi Informatique et Libertés trouve à s'appliquer. Ainsi, lorsqu'une automesure est réalisée manuellement, par exemple lorsqu'un individu relève manuellement le nombre de longueurs effectués lors d'une séance de natation, le fichier permettant de consigner les informations relevées devra présenter une certaine structure. Une certaine organisation devra effectivement être mise en place dans la retranscription des informations collectées afin que la qualification de fichier, à l'origine du déclenchement de la protection, puisse être appliquée. Entendue de manière large, la notion de traitement de donnée à caractère personnel permet donc d'englober un nombre important de situations dans lesquelles une opération est réalisée sur une donnée.

Cette définition élargie permet dès lors une application facilitée des principes protecteurs contenus au sein de la réglementation et qui contribuent à prendre en compte le parcours qui est réalisé par la donnée.

B. La prise en compte du parcours de la donnée

423. Les données personnelles, par nature volatiles en raison de leur immatérialité et de leur nombre important, risquent d'échapper à la maîtrise de l'individu auxquels elles se rapportent. Surtout, ce risque est renforcé par l'intensité des échanges entrepris dans le cadre de l'automesure connectée et par la diversité des mesures réalisées. Il est donc apparu nécessaire de faire en sorte qu'une fois créées et à disposition du responsable de traitement, ces données soient utilisées et traitées conformément à l'usage pour lequel elles avaient été collectées. Ainsi, cette maîtrise, qui est rendue possible par les capacités d'adaptation de la réglementation, se traduit concrètement par un encadrement du parcours de la donnée **(1)**, celui-ci étant également limité par l'application concrète du principe de minimisation des données collectées **(2)**.

1. La notion d'usage ultérieur compatible

424. La détermination du principe de finalité fait partie des obligations reposant sur le responsable d'un traitement de données personnelles. Ce principe de finalité est essentiel car c'est lui qui permet de déterminer en amont pour quels motifs une collecte de données personnelles est réalisée. La finalité, nécessaire pour délimiter l'usage qui sera fait des données personnelles, a notamment pour but d'assurer une certaine sécurité juridique aux individus. La personne concernée doit en effet pouvoir être en mesure de savoir quelle utilisation sera faite de ses données personnelles. Véritable raison d'être de la collecte, cette finalité déterminée contribue ainsi en théorie à la transparence et à la prévisibilité du traitement. Ces objectifs sont primordiaux en matière de *quantified-self*, en raison de la nature même des données collectées. L'exemple d'une société d'assurance développant une application de bien-être ou visant à doter ses assurés de *trackers* d'activité peut être avancé, cette société pouvant, en l'absence de finalité déterminée ou en cas de détournement de finalité, procéder à une discrimination tarifaire en fonction des habitudes de vie des individus[837].

Il semble pourtant important de ne pas négliger, et ce pour des raisons pratiques, le nécessaire équilibre entre l'impératif de protection des intérêts de la personne concernée par le traitement d'une part mais aussi le besoin d'accorder une certaine flexibilité aux responsables de traitement d'autre part. A travers la notion d'usage ultérieur compatible, la réglementation prévoit ainsi la possibilité d'une utilisation future et encadrée des données collectées. Il apparaît dès lors possible de distinguer entre la collecte immédiate de données personnelles et l'usage qui sera fait ultérieurement de ces données par le responsable de traitement. La notion de temporalité est essentielle, puisqu'on distingue entre la première opération matérialisée par la collecte et les opérations suivantes comme le stockage par exemple. Chaque traitement suivant la collecte, qu'il s'agisse de celui pour lequel la

[837] L'exemple de la société d'assurance AXA peut ici être avancé. Celle-ci a offert à des clients d'une offre d'assurance en santé un *tracker* d'activité et a fait bénéficier les assurés les plus actifs de bons de réduction pour des séances de médecine douce. Par ailleurs, la même société a développé une application de santé mobile destinée au marché espagnol et par laquelle elle permet aux individus de gagner des points leur permettant d'obtenir certaines réductions. Pour plus d'informations, voir notamment : Bernard Andrieu, « Traquer son bien-être et propriété des données : quel droit des sportifs 3.0 sur leur corps vivant ? », *JS*, 2016, n°162, p.36.

finalité a été déterminée à l'origine, ou les suivants, doit être considéré comme un traitement ultérieur.

425. L'exigence de compatibilité. Reprenant fidèlement les termes de l'article 6, 1°b de la directive 95/46/CE, l'article 6, 2° de l'ancienne version de la loi Informatique et Libertés avait posé un principe de comptabilité entre la finalité annoncée d'une collecte de données et les traitements ultérieurs qui pouvaient être réalisés. L'article 5 du Règlement général européen, en reprenant ce principe, interdit également tout traitement ultérieur qui serait incompatible avec les finalités liées à la collecte initiale. Le but est ainsi de pouvoir écarter le risque d'un usage injustifié des données. Mais, l'utilisation de ces dernières pour des finalités connexes doit être tolérée pour des questions pratiques, à condition de respecter le principe de compatibilité mis en œuvre. La Convention 108 du Conseil de l'Europe posait déjà ce principe en exigeant, sous la forme d'une double négation, que les données ne soient pas « traitées ultérieurement de manière incompatible avec ces finalités ».

Ainsi, le groupe de l'article 29 a indiqué que les fournisseurs de moteurs de recherche, en tant que responsables de traitement, « ne peuvent pas prétendre que leur but en collectant des données à caractère personnel est de développer de nouveaux services dont la nature est encore indéterminée »[838]. La finalité doit dès lors également permettre de déterminer dans « quelle mesure les données sont retraitées pour une autre finalité incompatible avec celle pour laquelle elles avaient été collectées à l'origine ». Surtout, le G29 a proposé dans un avis adopté en 2013 des critères relatifs à compatibilité d'un éventuel traitement ultérieur. Ce test de compatibilité, également repris à l'article 6, 4° du Règlement européen, a pour objectif que les données ne soient pas traitées pour des raisons fondamentalement différentes de la finalité annoncée[839]. Dès lors, un moteur de recherche annonçant traiter des données à caractère personnel pour des finalités statistiques ne pourraient par exemple légitimement fournir de telles données à des entreprises tierces à des fins commerciales.

[838] G29, Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche, 00737/FR, WP 148, adopté le 4 avril 2008.
[839] G29, Avis 03/2013 sur le principe de finalité, 00569/13/EN, WP 203, adopté le 2 avril 2013.

426. L'analyse formelle et substantielle. Les critères définis doivent permettre de déterminer si l'usage secondaire envisagé est compatible, « à travers une analyse préliminaire formelle qui peut suffire et dispenser de l'analyse substantielle »[840]. Par conséquent, si l'information initiale couvre dans sa formulation la finalité ultérieure, même implicitement, l'exigence de compatibilité sera remplie. En revanche, si tel n'est pas le cas, les différents critères relatifs à l'analyse substantielle doivent être analysés. Le G29 en avait défini quatre parmi lesquels on retrouvait le lien éventuel entre l'utilisation ultérieure et la finalité annoncée, le contexte dans lequel les données personnelles ont été collectées, la nature des données à caractère personnel ainsi que les mesures de protection pour assurer un traitement équitable et éviter tout impact indu sur les données personnelles. Le Règlement européen est venu en consacrer un autre, relatif aux éventuelles conséquences du traitement ultérieur sur les personnes concernées[841]. Une application de *running*, qui collecte des données relatives à la distance parcouru et au temps réalisé, pourra ainsi traiter ces données ultérieurement pour dispenser des conseils d'entraînement personnalisés. En revanche, l'usage ultérieur ne sera pas considéré comme compatible si le responsable de traitement entend procéder à un traitement pour déterminer les adresses des utilisateurs de l'application.

A défaut d'une telle compatibilité, le traitement ultérieur ne peut être mis en œuvre, même s'il peut s'appuyer sur l'un des fondements prévus par les articles 5 de la loi Informatique et Libertés réécrite et 6 du RGPD. Le G29 avait déjà indiqué que les exigences posées aux articles 6 et 7 de la directive de 1995 étaient cumulatives et qu'un responsable de traitement ne pouvait donc considérer le traitement ultérieur comme une nouvelle activité de traitement dont la légalité serait fondée par exemple sur la réalisation de l'intérêt légitime poursuivi par le responsable du traitement[842]. Surtout, la mise en œuvre d'un traitement ultérieur incompatible était et est toujours sanctionnée au titre du détournement de finalité, tel qu'incriminé par l'article 226-21 du Code pénal. Celui-ci vise non seulement le responsable de traitement mais surtout, « toute personne détentrice de données à caractère personnel à l'occasion de leur

[840] Matthieu Bourgeois, « Droit de la donnée, Principes théoriques et approche pratique », *Communication et commerce électronique*, LexisNexis, 2017, p. 76.
[841] Règlement (UE) 2016/679, article 6, 4°, d).
[842] G29, Avis 03/2013, *op. cit.*, p. 36.

enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement ».

427. Les exceptions. Certaines exceptions sont prévues par l'article 6, 4° du Règlement. En effet, certains types de traitements ultérieurs échappent à cette exigence de compatibilité, qu'il s'agisse de ceux fondés sur le consentement de la personne concernée ou de ceux fondés « sur le droit de l'Union ou le droit d'un Etat membre », dès lors que ce droit « constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, paragraphe 1 ». Dès lors, il peut être fait exception à cette exigence de compatibilité pour des motifs tenant par exemple à la sécurité ou à la défense nationale ou encore à la prévention et à la détection d'infractions pénales. La mention des traitements de données sensibles nécessaires à la recherche dans le domaine de la santé ou justifiées par l'intérêt public ne sont en revanche pas mentionnés par le Règlement, contrairement aux indications des précédentes versions de la loi de 1978. De plus, il existe dans certains cas une présomption de compatibilité du traitement, fondée sur le concept d'extension de finalité[843], notamment pour les cas de réutilisation à des fins statistiques ou à des fins de recherche scientifique ou historique[844].

2. Le principe de minimisation

428. Le recul du principe de proportionnalité. Le respect du principe de proportionnalité du traitement fait partie, au même titre que le principe de finalité précédemment évoqué, des obligations pesant sur le responsable de traitement. Ainsi, l'article 4 de la LIL dispose que les données à caractère personnel « sont adéquates, pertinentes et au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est nécessaire ». Reprenant le principe déjà énoncé par la directive de 1995 et par la Convention 108 du Conseil de l'Europe, mais absent du texte initial de la loi de 1978, le RGPD fait également mention de la proportionnalité en son article 5. Celle-ci est appréciée au regard des termes de la finalité avancée du traitement : « dérive de ce principe de finalité une règle de proportionnalité » ainsi que le soulignait Guy

[843] CNIL, 7ème rapport d'activité 1986, p. 43.
[844] Article 5. 1, b) et article 89 du Règlement (UE) 2016/679.

Braibant[845]. Cette règle n'est d'ailleurs pas explicitement mentionnée par les textes qui indiquent simplement que les données sont « adéquates, pertinentes et non excessives »[846], permettant d'exclure, par définition, une collecte de données pour un usage futur indéterminé ou aléatoire.

Le principe de proportionnalité, élément essentiel du dispositif protecteur des données, permet notamment d'avoir une influence sur la qualification des données collectées en contribuant notamment à la révélation de données relatives à l'état de santé[847]. Les modalités d'exposition de soi étant aujourd'hui amplifiées, notamment par le développement du *big data*, l'application concrète du principe de proportionnalité nécessite ainsi une vigilance particulière[848]. Le fait qu'un responsable de traitement puisse collecter des données qui soient sans rapport avec l'objet du traitement figure ainsi parmi les principaux risques d'atteinte à la personne concernée et il est nécessaire de s'assurer que les données collectées sont utiles à la poursuite de la finalité annoncée. L'exemple d'un pèse-personne connecté qui procèderait à la géolocalisation peut être avancé, la proportionnalité du traitement réalisé étant ici remise en cause par une collecte de données n'étant pas nécessaire au fonctionnement et à la délivrance du service attendu. La CNIL n'a pas eu à se prononcer directement en matière d'automesure connectée mais elle procède à un contrôle rigoureux de l'adéquation des données au regard de la finalité du traitement. Le cas de la géolocalisation des salariés a ainsi fait débat, notamment concernant la géolocalisation de véhicules de fonction[849], le dispositif ne pouvant par exemple pas conduire à contrôler la durée de travail des salariés[850].

429. Le passage au principe de minimisation. Le principe de proportionnalité, rendu difficile à appliquer par le développement de nouveaux

[845] Guy Braibant, *op. cit.*, p. 77.
[846] Exception faite du Règlement européen qui en fait la mention au considérant 156 et qui mobilise ce principe dans l'article 35 concernant l'analyse d'impact relative à la protection des données.
[847] Cf., *supra*, n° 202.
[848] Fabien Granjon, « Du (dé)contrôle de l'exposition de soi sur les sites de réseaux sociaux », *Les Cahiers du numérique*, 2014, Vol. 10, pp. 19-44.
[849] CNIL, Délibération n°2006-066 du 16 mars 2006 portant recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules autonomes utilisés par les employés d'un organisme privé ou public et CNIL, Délibération n° 2015-165 du 4 juin 2015 portant adoption d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés.
[850] Conseil d'Etat, 10e et 9e chambres réunies, 15 décembre 2017, n° 403776.

services aux finalités largement exprimées, laisse de plus en plus la place aujourd'hui à un principe de minimisation des données, auquel la proportionnalité était parfois déjà assimilée[851]. Cette référence à la minimisation est d'ailleurs explicitement mentionnée par le RGPD à l'article 5, 1° c) qui reprend le principe de proportionnalité. Dès lors, la minimisation des données n'a pas vocation à remplacer le principe de proportionnalité mais simplement à le compléter. En effet, à l'image du principe d'autodétermination informationnelle qui doit guider l'ensemble des éléments de protection mis en œuvre, le principe de minimisation des données collectées irrigue un certain nombre d'éléments protecteurs renouvelés ou instaurés par le RGPD. Notamment, celui-ci doit être pris en considération lorsque les instruments de conformité mis en place sont mobilisés, par exemple lors de la réalisation d'opérations de *privacy by design*[852].

Les principes de la réglementation protectrice des données personnelles, pour certains remis en cause par la pratique et les nouveaux moyens de collecte de données, ont tendance à être actualisés pour être adaptés aux nouveaux moyens de traitement. Ces principes, requis lorsqu'un traitement de données est mis en place, ont également vocation à s'appliquer lorsque les données collectées font l'objet de traitements ultérieurs.

§2. Une adéquation des principes aux cas de réutilisation

430. La loi Informatique et Libertés, de même que l'ensemble des autres textes à valeur contraignante visant à protéger les données personnelles des individus, ne repose pas sur une prohibition totale de l'utilisation des informations nominatives relatives aux individus. Tout au plus, celle-ci vise-t-elle à la conciliation d'intérêts différents, entre impératifs économiques pour certains responsables de traitement et protection des libertés individuelles pour les personnes dont les données font l'objet de telles opérations[853]. La nécessité de trouver un juste équilibre entre des intérêts

[851] Conseil d'Etat, *Le Numérique et Droits fondamentaux*, *op. cit.*, p. 168.
[852] Cf., *supra*., p. 126.
[853] Le second considérant de la directive de 1995 indique ainsi que les systèmes de traitement de données doivent « respecter les libertés et droits fondamentaux de ces personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ». De même, le règlement général indique dans son septième considérant vouloir « susciter

divergents repose dès lors sur la possibilité de maîtriser les hypothèses de réutilisation des données personnelles collectées et traitées. Si cette réutilisation est encadrée concernant les données simplement personnelles **(A)**, les données sensibles font l'objet d'une réutilisation strictement limitée **(B)**.

A. La Une réutilisation encadrée des données personnelles

431. La collecte de données personnelles est en soi susceptible de présenter un risque pour les individus, en raison du lien avéré existant entre informations nominatives et vie privée[854]. Le *quantified-self*, relatif à l'intimité des individus en raison de la nature des données collectées, de leur précision et de leur nombre, participe dès lors à ce mouvement de collecte exponentielle. Présentes dès l'origine avec le déploiement de l'informatique, les problématiques en cause se sont accrues avec le développement de l'automesure connectée. La loi Informatique et Libertés ainsi que le RGPD ont donc dû prendre en compte ces évolutions pour protéger les utilisateurs d'objets connectés ou d'applications d'interconnexions de fichiers **(1)**, tout en modérant les possibilités de réutilisation commerciale des données collectées **(2)**.

1. Les limites à l'interconnexion de fichiers

432. La loi Informatique et Libertés faisait référence à plusieurs reprises, avant sa réécriture, à la notion d'interconnexion de traitements ou de fichiers sans pour autant en donner de définition précise. Simplement, elle faisait d'abord figurer à l'article 2, alinéa 3, la notion de « rapprochement ou d'interconnexion » parmi les opérations susceptibles de constituer un traitement de données personnelles. Ensuite et conformément à l'article 30, 1, 3°, elle exigeait du responsable de traitement que celui-ci mentionne dans les formalités préalables « les interconnexions » et les « rapprochements » mais aussi « toutes autres formes de mises en relation avec

---

la confiance qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur », tout en permettant aux individus de bénéficier d'un « contrôle des données à caractère personnel les concernant ».

[854] Patricia Blanc-Gonnet Jonason, « Vers une meilleure adaptation du droit de la protection des données personnelles à la réalité informationnelle », *AJDA*, 2008, p. 2105.

d'autres traitements ». La version réécrite de la loi n'a pas retenu ces dispositions mais mentionne simplement que les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements doivent être précisés en cas de demande d'avis adressées à la CNIL. Cette dernière, en l'absence de définition, avait déjà eu l'occasion d'interpréter la notion dans une fiche pratique[855].

433. La notion d'interconnexion. Conformément à l'interprétation donnée par la CNIL, la notion d'interconnexion suppose, pour être retenue, la réunion de trois critères cumulatifs. Ainsi, l'objet de l'interconnexion doit être « la mise en relation de fichiers ou de traitements de données à caractère personnel », cette mise en relation devant concerner « au moins deux fichiers ou traitements distincts » et être constituée par « un processus automatisé ayant pour objet de mettre en relation des informations issues de ces fichiers ou de ces traitements ». La CNIL, tout en englobant la notion de « mise en relation » à celle d'interconnexion, retient une appréciation large de cette dernière. Les principaux critères retenus portent sur la nécessité d'interconnecter des données ayant spécifiquement un caractère personnel, sachant également que « l'interconnexion peut s'appliquer aux fichiers d'un même responsable de traitement ».

434. L'exclusion des simples rapprochements. La CNIL distingue les simples « rapprochements » des interconnexions. La CNIL distingue en revanche les simples « rapprochements » des interconnexions. En effet, elle considère que ceux-ci, s'ils constituent une forme de mise en relation[856], se distinguent de l'interconnexion du fait qu'ils ne sont pas nécessairement automatisés mais peuvent simplement résulter de « la comparaison visuelle d'informations issues de deux fichiers » ou encore de « l'enrichissement d'un fichier existant par saisie manuelle d'informations issues d'un autre fichier »[857]. Surtout, la CNIL indique explicitement que si un « rapprochement peut être réalisé au sein d'un même traitement ou fichier », l'interconnexion implique, en revanche, deux fichiers distincts.

[855] CNIL, *Comment déterminer la notion d'interconnexion*, Fiche pratique, 5 avril 2011.
[856] Anne Debet, Jean Massot, Nathalie Metallinos, *Informatique et Libertés*, *op. cit*., p. 465.
[857] *Ibid.*

La définition des différents critères relatifs à l'interconnexion présentait un intérêt pratique important en raison des contrôles susceptibles d'être portés sur ces opérations par la CNIL. En effet, si tous les traitements relatifs à une interconnexion n'étaient pas susceptibles de nécessiter une autorisation de la CNIL, celle-ci devait se prononcer, en vertu de l'ancien article 25, 1, 5°, sur les traitements automatisés ayant pour objet « l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents » ou ceux ayant pour objet « l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes ».

435. L'abandon des formalités préalables par le Règlement général a conduit à l'abrogation de ces dispositions. Pourtant, la dernière hypothèse mentionnée est certainement celle la plus susceptible de se présenter dans le cadre de la mise en place d'un dispositif d'automesure connectée. En effet, la quantité d'informations nominatives rendue disponible dans le cadre de l'automesure connectée par le recours aux objets connectés ou aux applications nécessite une vigilance particulière en cas d'interconnexion de fichiers. La question de l'interconnexion d'un fichier recensant « l'identité d'utilisateurs dont l'indice de masse corporelle a été calculé à partir des données remontées par une balance connectée avec le fichier client ou prospect d'un assureur » a ainsi pu être soulevé, l'intérêt légitime d'un tel traitement étant sujet à discussion[858]. Ainsi, l'interconnexion est susceptible d'aboutir à la création de nouveaux flux. Selon la CNIL, « des fichiers issus de deux traitements distincts peuvent être rapprochés ou comparés pour obtenir une information nouvelle ou la consolidation d'informations existantes ». Celle-ci devait auparavant autoriser de telles interconnexions lorsque les finalités principales des fichiers étaient différentes. Cette nécessité d'obtenir une autorisation a disparu, mais la CNIL a toujours à connaître des cas d'interconnexion lorsqu'elle doit rendre un avis en vertu de l'article 31 de la loi réécrite lorsque des traitements sont mis en œuvre pour le compte de l'Etat.

[858] Olivia Luzi, « Objets connectés et protection des données personnelles : le paradoxe », disponible en ligne à l'adresse : http://www.feral-avocats.com/fr/publication/objets-connectes-et-protection-des-donnees-personnelles-le-paradoxe/

Le RGPD procède, dans l'ensemble, à une simplification du dispositif protecteur applicable aux interconnexions. Celles-ci sont simplement mentionnées à l'article 4 du texte relatif aux définitions et relèvent ainsi des opérations constitutives d'un traitement de données. Malgré l'absence de dispositions spécifiques aux cas d'interconnexion, cette solution permet un meilleur encadrement de ces opérations puisqu'elles sont soumises aux dispositions renouvelées du RGPD et donc aux outils permettant de s'assurer de la conformité des traitements. Par ailleurs, les modalités de mise à disposition des informations en vue de leur réutilisation ont été précisées par le texte européen.

2. Une réutilisation commerciale modérée

436. L'utilisation des données personnelles représente, depuis les débuts du développement de l'informatique, une opportunité économique sans précédent. Outre les services en ligne proposés – achat d'applications ou de dispositifs connectés dans le cadre du *quantified-self* – les annonceurs bénéficient, avec les informations nominatives auxquelles ils peuvent avoir accès, de ressources leur permettant de proposer des publicités en ligne de plus en plus ciblées. Les données personnelles collectées constituent dès lors le socle de la prospection commerciale en ligne et la loi Informatique et Libertés modifiée pose, malgré certaines difficultés concrètes d'application[859], le cadre juridique applicable à une telle prospection. Outre cette problématique particulière, la question de l'*open data* doit également être mentionnée afin d'expliciter les cas de mise à disposition des données, éventuellement identifiantes, ainsi que les limites qui sont aujourd'hui apportées aux cas de réutilisation commerciale de telles informations.

437. Des domaines théoriquement éloignés. Le *quantified-self* et l'ouverture des données publiques sont des domaines qui ont eu tendance à se développer de façon séparée. Pourtant, des éléments de convergence entre les problématiques relatives à la réutilisation des informations publiques et à la protection des données personnelles ont progressivement vu le jour et des interactions entre les deux matières

[859] Cf., *supra*, n° 287.

ont été inévitables[860]. Les informations publiques, mises à disposition par l'administration sous forme de données numériques et entendues par le G29 comme « toutes les informations du secteur public accessibles au public en vertu du droit national »[861] ont de plus en plus été appelées à contenir des informations relatives aux individus. Les limites relatives à l'apport des données d'automesure aux informations publiques et à leur réutilisation ont déjà été soulevées[862]. Mais le renouvellement des législations applicables aux données publiques d'une part et aux données à caractère personnel d'autre part laisse entrevoir une meilleure prise en compte des problématiques relatives à la vie privée, notamment au stade de la réutilisation des informations publiques.

438. Les rapprochements progressifs. En France, les acteurs publics ont rapidement pris conscience de la nécessité d'encourager le développement du mouvement d'ouverture des données publiques. Une mission, Etalab, a été créée en 2011 afin de favoriser et de coordonner la récolte de données publiques au sein des différentes administrations de l'Etat. Celle-ci s'inscrit dans un mouvement plus général de développement de la politique publique d'ouverture et prend place au sein d'une « kyrielle de structures ad hoc »[863] visant à soutenir la mise en œuvre d'une politique cohérente de mise à disposition des données. Le RGPD accompagne cette transition en renouvelant profondément les règles relatives à la protection des données à caractère personnel. Également applicables aux personnes publiques, ce texte doit permettre une réutilisation facilitée des informations détenues par les administrations et ainsi favoriser le développement de nouvelles opportunités pour le mouvement d'ouverture et de réutilisation des données.

439. La consécration par le RGPD. Le RGPD intègre la mise à disposition dans son champ de protection et assimile celle-ci à un traitement en vertu de l'article 4 du texte. Le considérant 154 du Règlement mentionne explicitement la question des rapports entre *open data* et protection des données personnelles pour les cas de réutilisation des données libérées. Celui-ci insiste sur la nécessité de concilier « la

[860] Gaëtan Gorce, François Pillet, *La protection des données personnelles dans l'open data : une exigence et une opportunité*, Rapport d'information du Sénat fait au nom de la commission des lois, n°469, 2014, p. 25.
[861] G29, Avis 06/2013, *op. cit*., p. 2.
[862] Cf., *supra*, n° 199.

réutilisation des informations du secteur public, d'une part, et le droit à la protection des données à caractère personnel, d'autre part »[864]. La mise en œuvre de traitement de données à caractère personnel obtenues par suite de la mise à disposition par les administrations doit donc respecter les dispositions protectrices renouvelés du Règlement, qu'il s'agisse de la nécessité d'obtenir un consentement préalable renforcé[865] ou de l'obligation d'informer qui pèse sur le responsable de traitement. Ce renouveau du cadre juridique applicable aux données à caractère personnel, complété par l'adoption de la directive du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public[866], doit permettre une meilleure protection des informations. Mais il doit aussi favoriser la standardisation des données traitées. Le fait que celles-ci soient généralement désorganisées et regroupées dans des formats différents constitue encore aujourd'hui un frein aux mécanismes de l'ouverture des données publiques.

Les données d'*open data* constituent en effet, pour les personnes appelées à réutiliser les données libérées, un matériau riche permettant la création de nouveaux services. Les liens entre automesure connectée et *open data* sont encore minces aujourd'hui[867]. Cependant, la politique d'ouverture des données publiques, fondée sur la possibilité d'accéder et de réutiliser librement et gratuitement l'information, s'inscrit dans une perspective large[868]. Le renouvellement presque simultané des cadres juridiques applicables à la protection des données et à l'ouverture des données publiques pourra, après un certain temps d'adaptation, contribuer au développement d'une culture partagée de la protection des données, entre innovateurs et administrations. Une telle dynamique, qui permet notamment de prévoir en amont les cas de réutilisation d'informations publiques dans la mise en œuvre de dispositifs d'automesure, serait alors semblable à celle ayant eu lieu en 1978 et ayant donné

---

[863] Philippe Yolka, « Le droit de l'immatériel public », *ADJA*, 2017, p. 2047.
[864] Considérant 154 du Règlement (UE) 2016/679.
[865] Laure Marino, « Le règlement européen sur la protection des données personnelles : une révolution ! », *La Semaine Juridique*, Edition générale, n°22, p. 6.
[866] Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public.
[867] Cf., *supra*, n° 359.
[868] Henri Verdier, Suzanne Vergnolle, « L'Etat et la politique d'ouverture en France », *AJDA*, 2016, p. 92.

naissance à un cadre protecteur des données et à un mouvement de transparence de l'action administrative.

B. La réutilisation limitée des données de santé

440. L'automesure connectée contribue à la création de données relatives à la santé et qui sont donc traditionnellement soumises au régime juridique des données sensibles. A ce titre, les modalités de collecte de ces données sont encadrées et limitées et les modalités de réutilisation et de traitements ultérieurs de ces données sont également restreintes. En effet, les risques relatifs à la vie privée étant amplifiés en raison de la sensibilité des informations collectées, le but est de protéger ces données contre d'éventuelles utilisations commerciales **(1)** ce qui permet de justifier que l'exploitation soit majoritairement maitrisée par des entités publiques **(2)**.

1. Une protection contre les utilisations commerciales

441. Différentes règles sont susceptibles de s'appliquer pour protéger les données sensibles de la prospection commerciale. En effet, les dispositions de la loi Informatique et Libertés et du RGPD sont dans certains cas complétées par des textes spéciaux. Le Code de la santé publique dispose par exemple que « sont interdites la constitution et l'utilisation à des fins de prospection ou de promotion commerciales de fichiers composés à partir de données issues directement ou indirectement des prescriptions médicales ou des informations médicales mentionnées à l'article L.161-29 du Code de la sécurité sociale, dès lors que ces fichiers permettent d'identifier directement ou indirectement le professionnel prescripteur »[869]. Sont dès lors concernés « le numéro de code des actes effectués, des prestations servies à ces assurés sociaux ou à leurs ayants droit »[870].

442. Le domaine des assurances. Le domaine des assurances entretient un lien particulier avec le *quantified-self*. Les données récoltées par les objets connectés, notamment les données relatives à la santé, constituent en effet une ressource d'une

[869] Article L. 4113-7 du CSP.
[870] Article L. 161-29 du CSP.

grande valeur pour les assureurs. Ces derniers seraient donc susceptibles, en y ayant accès, d'adapter les tarifs de leurs polices d'assurance en fonction des informations qu'ils ont à leur disposition. Un individu jeune, actif, sportif et en bonne santé pourrait ainsi bénéficier de tarifs avantageux. A l'inverse, une personne dont les objets connectés révéleraient qu'elle a une alimentation moins équilibrée, pratique moins d'activités physiques ou souffre d'arythmie cardiaque, pourrait se voir proposer des tarifs plus élevés en raison des risques plus importants qu'elle présente pour la compagnie d'assurance. Les données de santé traitées grâce aux objets connectés seraient donc source de discriminations envers les individus en cas d'exploitation non contrôlée de celles-ci. Une proposition de loi déposée en janvier 2019 entend justement interdire l'usage des données personnelles collectées par les objets connectés dans le domaine des assurances[871]. Tout en rappelant que les données traitées dans le cadre du *quantified-self* peuvent « à l'occasion être une aide supplémentaire à destination du corps médical », cette proposition de loi « suggère d'interdire aux compagnies d'assurance d'utiliser et de traiter de telles informations » et ce afin de « remédier aux abus dans le champ de l'assurance vie et de l'assurance maladie ».

443. Le domaine de la consommation. Outre cette hypothèse particulière, les éventuelles revendications commerciales qui pourraient apparaître en matière de données sensibles doivent respecter le droit commun relatif à la protection des données personnelles. Selon l'article 6 de la LIL réécrite, le traitement de données sensibles est en principe interdit. Certaines exceptions sont cependant prévues par le texte, à l'image du consentement de la personne. Une telle exception a vocation à s'appliquer au domaine du *quantified-self*, l'individu étant en mesure de s'opposer, selon les modalités précédemment étudiées, à l'utilisation de ses données personnelles sensibles à des fins de prospection commerciale. Cette condition du respect des dispositions relatives au traitement des données sensibles, si elle montre bien qu'aucune disposition particulière n'empêche le traitement et l'utilisation de

[871] Proposition de loi n° 1603 visant à interdire l'usage des données personnelles collectées par les objets connectés dans le domaine des assurances.

telles données, ne doit pas faire oublier la condition relative au respect du secret médical[872].

Le traitement des données sensibles est aujourd'hui strictement encadré. Les modalités de réutilisation de telles informations, contrôlées par des entités publiques, font également l'objet d'un encadrement précis.

2. Le contrôle de la réutilisation

444. Le droit commun de la protection des données personnelles relatif à la prospection commerciale a, par nature, vocation à s'appliquer aux données issues d'objets connectés utilisés dans le domaine de la santé. Dès lors, les sociétés proposant de telles solutions, soumises aux dispositions de la loi de 1978 modifiée et réécrite, ont l'obligation de restreindre les modalités d'accès et de réutilisation des données qu'elles ont à leur disposition. Une solution similaire, bien que renforcée, a également vocation à s'appliquer aux données personnelles collectées et détenues par les personnes publiques. Contenues à l'origine dans différentes bases de données gérées de manière séparée, les modalités d'accès à ces informations ont fait l'objet d'une importante réforme visant à en faciliter l'accès.

445. Les bases de données de santé. La loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé a permis la création d'un Système National des Données de Santé dont le but est de regrouper les principes bases de données de santé publiques existantes. A ce titre, y sont regroupées des bases telles que celle du SNIIRAM concernant les données de l'assurance maladie, celle dite PMSI concernant les données issues de l'activité des établissements de santé, la base CepiDC regroupant les données sur les causes de décès, les données liées au handicap issues de maisons départementales des personnes handicapées (MDPH) et enfin, les données provenant des complémentaires santé. L'éventail large des données contenues au sein de ce système national, détaillé au sein de l'article R.1461-4 du Code de la Santé publique doit servir à « réformer l'accès aux données de santé afin que leurs

[872] Didier Houssin, « Le secret médical dans les nouvelles pratiques et les nouveaux champs de la médecine », *Recueil Dalloz*, 2009, p. 2619.

potentialités soient utilisées au mieux dans l'intérêt de la collectivité et du principe de valeur constitutionnelle de protection de la santé » tout en assurant « la confidentialité des données personnelles qui procède du droit au respect de la vie privée »[873].

446. La mise à disposition. L'article L. 1461-2 du Code de la santé publique prévoit ainsi la mise à disposition gratuite pour le public de jeux de données et l'article 193 de la loi de modernisation de notre système de santé insiste dès lors sur la nécessité que la mise à disposition des données de santé à caractère personnel recueillies ne puisse « en aucun cas avoir pour fin l'identification directe ou indirecte de ces personnes »[874]. L'article L. 1461-4 indique à cette fin que « le système national des données de santé ne contient ni les noms et prénoms des personnes, ni leur numéro d'inscription au répertoire d'identification des personnes physiques, ni leur adresse ».

L'accès à certaines bases de données était au départ interdit aux acteurs du secteur privé – dans le cas du SNIIRAM notamment. Mais la loi de modernisation de notre système de santé a retenu une solution inverse, sous certaines conditions. En effet, la finalité de l'exploitation des données prévaut désormais sur le « statut juridique de l'utilisateur »[875]. L'accès des données au secteur privé est encadré par la liste limitative des finalités susceptibles d'être invoquées, à l'exclusion des fins de promotion des produits de santé et des fins d'exclusion de garanties des contrats d'assurance ou la modification des cotisations et des primes d'assurance.

447. Le lien entre automesure et santé publique. Le lien entre mise à disposition de données agrégées de santé au public, objets connectés et *quantified-self* peut sembler ténu. Pourtant, des hypothèses de rapprochement sont particulièrement envisageables. En effet, les données de santé contenues au sein des bases médico-administratives sont créées dans le cadre des parcours de soins traditionnels, faisant intervenir des personnes soumises au secret médical. Mais, d'autres données sont

[873] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, Exposé des motifs.
[874] Article L. 1460-1 du CSP.
[875] Cour des comptes, *Les données personnelles de santé gérées par l'assurance maladie, Une utilisation à développer, une sécurité à renforcer*, Communication à la commission des affaires sociales et à la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale de l'Assemblée nationale, mars 2016, p. 97.

collectées en dehors de ces systèmes, à l'occasion de multiples activités humaines (réseaux sociaux, objets connectés, applications…)[876]. Ainsi, l'inclusion de ce qui a pu être qualifié de donnée de vie réelle, « générées à l'occasion des soins réalisés en routine pour un patient, et qui reflètent donc la pratique courante », provenant également d'objets connectés, permettrait éventuellement d'optimiser l'usage des bases disponibles[877]. Une telle hypothèse, étudiée outre-Atlantique[878], pourrait prochainement faire son apparition en France. La loi du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé entend en effet aller plus loin que la loi de modernisation de notre système de santé du 26 janvier 2016. Ce nouveau texte vise d'abord à élargir les données du SNDS à l'ensemble des données cliniques obtenues dans le cadre de soins remboursés par l'Assurance maladie, pour contribuer à mettre en place une nouvelle « Plateforme des Données de santé ». Ensuite, cette nouvelle loi devrait également permettre l'intégration de données issues de dispositifs connectés, objets ou applications, au sein d'un nouvel « espace numérique de santé », ouvert automatiquement pour chaque individu. Il serait ainsi possible d'imaginer, à terme, que les données issues d'objets connectés d'automesure puissent être intégrées aux données de la nouvelle « Plateforme des Données de santé », renforçant ainsi le lien entre automesure et mise à disposition des données.

448. Conclusion du chapitre. Les données à caractère personnel traitées dans le cadre du *quantified-self* font l'objet d'un nombre important d'opérations qui impliquent que les données soient transférées entre différents acteurs. Ces éléments, rendus nécessaires par les spécificités des traitements d'automesure et l'enrichissement permanent dont celles-ci font l'objet, ont progressivement été pris en compte par la réglementation. Celle-ci a en effet évolué pour s'adapter à ces nouvelles pratiques. Les définitions employées par les textes ont été précisées pour identifier plus facilement les différents opérateurs – responsables de traitement, sous-traitant, sous-traitant ultérieur – et les principes de protection mis en œuvre – principe de finalité ou de proportionnalité – ont évolué, permettant de mieux saisir la réalité

[876] Bernard Bégaud, Dominique Polton, Franck von Lennep, L*es données de vie réelle, un enjeu majeur pour la qualité des soins et la régulation du système de santé, L'exemple du médicament*, Rapport réalisé à la demande de Madame la Ministre de la santé Marisol Touraine, Rapport final, mai 2017, p. 47.
[877] *Ibid*.
[878] Emil Chiauzzi, Carlos Rodarte, Pronabesh DasMahapatra, « Patient-centered activity monitoring in the self-management of chronic health conditions », *BMC Medicine*, 2015, p. 13 à 77.

actuelle des traitements. Outre le recours à différents prestataires, la pratique de l'automesure connectée a également entraîné un accroissement des transferts internationaux de données, les différents opérateurs mobilisés se trouvant généralement dans des zones géographiques dispersées.

CHAPITRE II – LA PRISE EN COMPTE DES EXTERNALISATIONS GÉOGRAPHIQUES

449. L'automesure connectée repose sur une interaction entre plusieurs acteurs, responsables de traitements, sous-traitants et destinataires par exemple. Mais la mise en œuvre de dispositifs de *quantified-self* repose également sur une expansion territoriale du cadre de traitement des données à caractère personnel. La connexion à Internet des objets utilisés permet un partage de données entre différents opérateurs et elle fait appel au caractère mondialisé des échanges. En effet, la diversité des capteurs utilisés dans le cadre de l'automesure connectée semble faciliter, en raison de leur développement massif, ces transferts internationaux. Dès lors, ceux-ci s'intègrent dans un espace sans frontière ni attaches géographiques précises et ils sont susceptibles d'être concernés par différentes réglementations nationales. Ainsi, un individu ayant recours à un podomètre connecté pourra par exemple voir ses mesures collectées par une société française, qui les fera analyser par un sous-traitant russe et qui pourra ensuite les stocker aux Etats-Unis. La question se pose dès lors de savoir quelle réglementation appliquer.

450. Le développement du numérique dans notre société pose un certain nombre d'interrogations, particulièrement concernant l'appréhension juridique du territoire. En effet, le numérique met en évidence « deux approches de l'espace : l'espace territorial du droit et ce qu'il est convenu d'appeler le cyberespace, pour lequel les frontières géographiques importent peu »[879]. Oscillant donc entre lieu et identité[880], « le cyberespace se présente comme un environnement dépourvu de plusieurs des repères sur lesquels se fondaient habituellement les normativités » et il « défie les repères que sont les frontières des Etats, cadres privilégiés du droit » tout en ayant pour effet de rendre « les frontières nationales transparentes »[881]. Ce faisant,

[879] Cyril Rojinsky, « Cyberespace et nouvelles régulations technologiques », *Recueil Dalloz*, 2001, p. 844.
[880] Alix Desforges, « Les représentations du cyberespace : un outil géopolitique », *Hérodote*, vol. 152-153, no. 1, 2014, pp. 67-81.
[881] Pierre Trudel, « Quel droit et quelle régulation dans le cyberespace ? », *Sociologie et sociétés*, Volume 32, numéro 2, 2000, p. 191.

il devient complexe de pouvoir fixer géographiquement une réglementation dans un monde qui est, par définition, ouvert. Le risque est en effet de soumettre les données des individus à des réglementations nationales fragmentées. Pourtant, au vu des enjeux en question, l'exercice effectif de la réglementation apparaît comme la garantie nécessaire des libertés individuelles.

451. L'Internet, « prôné ou fantasmé par certains comme un espace sans entrave, affranchi des contraintes du monde « réel », était censé puiser dans son immatérialité sa méconnaissance des frontières »[882]. Pourtant, il a fallu mettre en œuvre des solutions garantissant les droits et libertés des individus, en quelque endroit qu'ils puissent se trouver. Relative à une extension de la compétence territoriale ou à un encadrement des transferts internationaux de données, les règles mises en œuvre ont cherché à encadrer l'internationalisation des échanges rendus possibles et à en limiter les risques pour les individus. Loin de vouloir limiter ces transferts de données, la réglementation déployée a simplement cherché à intégrer la réalité de l'inexistence des frontières en permettant une meilleure traçabilité des données collectées.

Cette traçabilité des données est devenue difficile ces dernières années, notamment en raison de l'apparition et du développement des solutions de *cloud-computing*. Dénommée informatique en nuage en français, le *cloud* repose sur le stockage à distance des informations traitées par l'intermédiaire d'une connexion à un réseau et par l'emploi de serveurs informatiques. Parfois perçu comme « occulte »[883] en raison des différents moyens techniques mis en oeuvre, le stockage réalisé grâce à ce type de procédé est surtout susceptible de constituer une externalisation supplémentaire pour les données collectées. Entre coûts réduits et facilité d'utilisation, le *cloud-computing* a été massivement employé par les entreprises et les administrations pour répondre à leurs besoins en matière d'hébergement de données. Cette solution est pourtant porteuse de questions et de risques juridiques, que ce soit au niveau de la gouvernance des données hébergées ou même de l'emplacement des

[882] Agathe Lepage, « Droit pénal et internet : la part de la tradition, l'oeuvre de l'innovation », *AJ pénal*, 2005, p. 217.
[883] Antoine Gendreau, « La dématérialisation du dépôt : l'exemple du contrat de cloud computing », *AJ contrat*, 2016, p. 519.

données stockées, celui-ci n'étant pas toujours porté à la connaissance du client ayant recours à une telle prestation[884].

452. Le *quantified-self* est susceptible d'entraîner des transferts géographiques et extraterritoriaux de données personnelles et les services qui sont proposés dans ce cadre peuvent conduire à des interactions avec des prestataires situés hors du lieu de résidence de la personne concernée par un traitement de données personnelles. De même, les responsables de traitement peuvent avoir recours à une solution d'hébergement décentralisée pour le stockage de ces données. Un doute peut dès lors survenir quant à l'application territoriale de la loi et à l'effectivité des mesures de protection mises en œuvre et l'individu concerné par de tels traitements peut perdre la maîtrise de ses données personnelles en raison notamment d'un manque de transparence quant aux lieux où ses données sont transférées ou stockées. Pourtant, ce risque apparent de délocalisation des données personnelles **(section 1)** est en principe tempéré par une expansion territoriale du cadre juridique applicable à de telles données **(section 2)**.

[884] Geoffray Brunaux, « Cloud computing, protection des données : et si la solution résidait dans le droit des contrats spéciaux ? », *Recueil Dalloz*, 2013, p. 1158.

SECTION I. LE RISQUE APPARENT DE DÉLOCALISATION DES DONNÉES PERSONNELLES

453. Les impératifs économiques en jeu, notamment dans le cadre du *quantified-self*, reposent sur la nécessité, à l'ère de la globalisation de l'information et du bouleversement des médias traditionnels, de faire transiter de telles données. Les services d'automesure connectée, qu'ils soient proposés par les plus grandes compagnies américaines en complément de leurs services principaux ou par d'autres compagnies spécialisées, déploient leurs moyens de collecte à travers la planète. Cependant, une fois les données transférées hors des frontières, le régime de protection nationale n'a plus exclusivement vocation à s'appliquer et la protection des données à caractère personnel peut en partie reposer sur la réglementation du pays destinataire des données[885]. Des garanties permettant à l'individu de garder la maîtrise sur ses données personnelles ont alors dû être mises en place, non sans résistance, comme en témoignent les solutions de compromis qui en résultent.

A ce titre, il semble en effet nécessaire de rappeler que l'ensemble de la réglementation relative à la protection des données personnelles repose aujourd'hui sur un équilibre impératif entre d'une part, liberté de circulation des données et d'autre part, protection des droits des individus. Ainsi, plutôt que d'interdire toute possibilité de transferts de données au niveau international, il a fallu trouver une solution permettant de procéder à certains transferts. Le but a ainsi été de pouvoir encadrer les éventuels transferts internationaux de données, sans pour autant en interdire purement et simplement toute possibilité. Cet encadrement, aujourd'hui fondé sur la notion du niveau de protection adéquat **(Paragraphe 1)**, a pourtant été confronté au développement massif de solutions reposant sur le recours à l'informatique en nuage **(Paragraphe 2)**.

[885] Anne Debet, Jean Massot, Nathalie Metallinos, *op. cit.*, p. 648.

§1. Le principe du niveau de protection adéquat

454. Le chapitre XII de la loi Informatique et Libertés faisait, avant sa réécriture, expressément référence aux cas de transferts de données à caractère personnel vers des Etats n'appartenant pas à la communauté européenne. Cette solution, fondée sur le principe de libre circulation des données au sein de l'espace économique européen, s'expliquait notamment par le rapprochement entre les différentes législations européennes opéré par la directive. Cette dernière, dans son article premier, rappelait l'obligation pour les Etats membres d'assurer « 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 ». Les Etats assuraient dès lors une protection équivalente en vertu de la directive et le transfert de données vers un pays tiers ne pouvait être réalisé que si celui-ci assurait un niveau de protection « adéquat » au sens de l'article 25 du même texte. Repris sous l'appellation de niveau de protection suffisant par le texte de la loi de 1978 modifié, celui-ci vise à encadrer les transferts internationaux de données **(A)**. A ce titre, l'encadrement des transferts outre-Atlantique présente certaines particularités **(B)**.

A. L'encadrement des transferts internationaux de données

455. La directive de 1995 et après elle, le Règlement général relatif à la protection des données, ont eu pour but de créer un cadre commun de protection autorisant que des transferts de données soient réalisés entre les Etats membres. La question de l'encadrement desdits transferts s'est posée concernant les pays tiers à l'Union et elle a dès lors nécessité la mise en œuvre de certaines mesures protectrices. Le but étant, pour l'individu, que celui-ci se voit accorder un niveau de protection équivalent de ses données, peu importe l'endroit où celles-ci sont transférées. Ainsi, la règlementation autorise les transferts vers des pays tiers présentant un niveau de protection suffisant **(1)** mais elle interdit en principe que de tels transferts soient réalisés en l'absence de cette garantie **(2)**.

1. Les transferts vers les pays offrant un niveau de protection adéquat

456. L'absence de définition légale du transfert. La notion de transfert de données à caractère personnel semble connaître une acceptation large. Pourtant, celle-ci n'a jamais été précisément définie par les différents textes successifs, qu'il s'agisse précédemment de la directive de 1995 ou désormais du RGPD et de la LIL modifiée et réécrite. Tout au plus, la version originale de cette dernière prenait en compte « la transmission entre le territoire français et l'étranger, sous quelque forme que ce soit, d'informations nominatives traitées ». Le régime relatif aux transferts de données a par la suite été intégré au sein de l'article 68 de la loi Informatique et Libertés modifié qui est devenu, grâce à la réécriture du texte, l'article 123 du texte. Celui-ci indique en son alinéa premier que « le responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat n'appartenant pas à l'Union européenne que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet ».

457. L'interprétation de la notion. Au regard de cette définition, la CNIL a interprété, avant l'adoption du Règlement, la notion de transfert. Elle a indiqué que l'on parle de transfert de données à caractère personnel « lorsque ces données sont transférées depuis le territoire européen vers un ou des pays qui n'appliquent pas les dispositions de la directive 95/46/CE », en précisant qu'il ne s'agit ni des pays membres de l'Union européenne, ni de ceux membres de l'Espace économique européen[886]. La zone territoriale concernée par la notion de transfert, définie par exclusion, a été entendue largement tout comme les modalités selon lesquelles un transfert pouvait être réalisé. La CNIL a en effet indiqué que ce transfert pouvait être effectué « par communication, copie ou déplacement de données, par l'intermédiaire d'un réseau ou d'un support à un autre, quel que soit le type de support », relevant ainsi l'indifférence du moyen utilisé pour le transfert.

Outre la nécessité que le destinataire des données transférées soit dans un pays tiers et qu'un transfert soit effectivement opéré, les différents textes successifs ainsi

[886] CNIL, *Les transferts de données à caractère personnel hors Union européenne*, novembre 2012, p. 5.

que la dernière itération de la loi Informatique et Libertés relèvent que les données transférées peuvent éventuellement faire l'objet d'un traitement postérieur au transfert. L'article 25 de la directive 95/46/CE distinguait entre les cas où le traitement était réalisé en amont du transfert et les cas où ce dernier était un préalable au traitement et le RGPD reprend à son compte cette distinction, au sein de son article 44. Dans certains cas en effet, le transfert porte sur des données déjà traitées alors que dans d'autres cas, les données sont transférées pour ensuite faire l'objet d'un traitement. La CNIL avait cependant relevé de manière générale que si le transfert ne constitue pas en soi un traitement autonome, il constituait néanmoins un traitement de données à caractère personnel « soumis à l'ensemble des dispositions de la loi du 6 janvier 1978 modifiée »[887]. A ce titre, la notion de transfert devait être précédemment distinguée de celle relative au transit d'une donnée. Mentionné au sein de l'ancien article 30 de la loi de 1978, ce transit signifiait seulement un passage des données via un serveur et celui-ci n'impliquait « aucun accès ou manipulation des données » [888] et n'était donc pas constitutif d'un traitement. Cette distinction propre au simple transit des données n'a pourtant pas été reprise par le RGPD et par la LIL qui précise simplement en son article 123 qu'un responsable de traitement ne peut transférer des données à caractère personnel vers un Etat n'appartenant pas à l'Union européenne.

458. Le niveau de protection suffisant. Cette affirmation est toutefois tempérée par la référence au niveau de protection suffisant qui est accordé aux données transférées. La directive de 1995 faisait référence à la notion de protection adéquate en listant les éléments qui permettaient d'apprécier ledit caractère adéquat d'un transfert de données. Plus exhaustive sur ce point que la loi de 1978, elle indiquait que l'adéquation devait « s'apprécier au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données ». Plusieurs éléments étaient ensuite évoqués, tels que la « nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesure de sécurité qui y sont respectées ».

[887] *Ibid.*, p. 6.
[888] Anne Debet, Jean Massot, Nathalie Metallinos, Informatique et Libertés, *op. cit.*, p. 659.

459. Une appréciation *in concreto*. Le principe d'adéquation ou de protection suffisante suppose une appréciation *in concreto* des mesures protectrices mises en œuvre par un Etat tiers. Cette appréciation doit notamment porter sur le fait que « les principes majeurs de la protection des données soient effectivement mis en œuvre dans le droit interne de ce pays »[889]. La directive de 1995 et la loi de 1978 modifiée présentaient chacune un faisceau d'indices quant aux éléments méritant une attention particulière, finalité et durée du traitement par exemple. En se fondant sur ces textes, le groupe de l'article 29 avait proposé une doctrine sur cette thématique, visant à déterminer les mécanismes de vérification de l'adéquation. Cette méthodologie portait, de manière générale, sur l'appréciation des principes fondamentaux de la réglementation relative à la protection des données personnelles, entre obligations à respecter de la part du responsable de traitements et garanties à apporter aux personnes concernées par de tels traitements[890].

460. La décision d'adéquation. Cette appréciation du caractère adéquat ou suffisant de la protection mise en œuvre par un pays tiers débouchait sur l'adoption, par la Commission européenne, d'une décision d'adéquation. Le constat de cette adéquation était de la compétence en théorie exclusive de la Commission. Mais les Etats membres disposaient de certains pouvoirs limités d'intervention, matérialisés notamment par un mécanisme d'information mutuelle consacré à l'article 25 alinéa 3 de la directive. Ce rôle d'alerte conféré aux Etats permettait notamment à la CNIL, sur le fondement de l'ancien article 70 alinéa 2 de la loi Informatique et Libertés, de constater provisoirement la non-adéquation de la législation d'un Etat n'appartenant pas à la Communauté européenne, en attendant l'avis définitif de la Commission. En tout état de cause, la décision d'adéquation publiée par la Commission au Journal Officiel de l'Union européenne entraînait la liberté du transfert entre les pays de l'Union et le pays dont la législation avait été reconnue comme adéquate. Une liste blanche de pays présentant un niveau de garantie suffisant a ainsi été publiée. Relativement restrictive, elle ne concernait qu'une dizaine d'Etats.

---

[889] Agence des droits fondamentaux, *Manuel de droit européen en matière de protection des données*, 2014, p. 215.
[890] G29, Document de réflexion du 26 juin 1997, *Premières orientations relatives aux transferts de données personnelles vers des pays-tiers – Méthodes possibles d'évaluation du caractère adéquat de la protection*, WP 4, p. 6.

461. Des mécanismes confirmés par le RGPD. Le Règlement général européen reprend peu ou prou les mêmes mécanismes en indiquant qu'un transfert vers un pays tiers ou une organisation internationale peut avoir lieu « lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat »[891]. L'article 45 alinéa 2 du texte précise les éléments que la Commission prend en considération lorsqu'elle évalue le caractère adéquat du niveau de protection. Par ailleurs, un mécanisme d'examen périodique est mis en œuvre par le texte, permettant de s'assurer de la continuité du caractère adéquat des mesures protectrices mises en œuvre par le pays tiers. Outre ces modalités de transfert, des dispositions sont également prévues par la réglementation dans le cas où le transfert est réalisé à destination d'Etats n'ayant pas fait l'objet d'une décision d'adéquation.

2. Les transferts vers les autres pays

462. Les transferts à destination d'Etats tiers peuvent être autorisés à titre général par des décisions d'adéquation de la Commission et le principe reste celui de l'interdiction de tout transfert lorsqu'une telle décision n'a pas été constatée. Cette interdiction de transférer des données était auparavant sanctionnée par un certain nombre de mesures, administratives ou pénales. En effet, la CNIL pouvait tout d'abord exercer son pouvoir de sanction à l'encontre des opérateurs ayant procédé à un transfert de données sans respecter les formalités préalables nécessaires. L'abandon du régime relatif aux formalités préalables par le Règlement européen a cependant entraîné un changement dans la mise en œuvre de ce pouvoir de sanction. Le non-respect des dispositions relatives au transfert est désormais intégré à l'article 83 du texte qui prévoit des sanctions renouvelées pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial total de l'exercice précédent. Des dispositions pénales permettent également de sanctionner la mise en œuvre de transferts illicites. L'article 226-16 du Code pénal précise encore que le fait de procéder à un traitement sans respecter les formalités préalables nécessaires pour tout

[891] Article 45 du Règlement (UE) 2016/679.

traitement est puni par la loi de cinq ans d'emprisonnement et de 300 000 euros d'amende. Par ailleurs, l'article 226-22-1 du même Code sanctionne désormais précisément les cas de transferts effectués en « violation du chapitre V du règlement (UE) 2016/679 du Parlement européen et du Conseil ».

463. L'inadéquation au cas du *quantified-self*. La procédure mise en œuvre pour la vérification de l'adéquation de la législation d'un Etat tiers semble en apparence peu adaptée aux nouvelles capacités techniques des outils aujourd'hui développés, notamment dans le cadre du *quantified-self*. Le but de l'automesure connectée est de procéder à des comparaisons, de corréler des données issues d'instruments de mesure différents ou encore de procéder à une analyse de ces données par différents opérateurs, en vue d'obtenir un retour d'informations le plus précis et le plus personnalisé possible. La véritable valeur d'usage du service repose ainsi sur l'échange constant de données par la connexion à Internet quasi-permanente des dispositifs utilisés, ce qui permet un transfert systématique de données vers des pays qui sont parfois situés hors de l'Union européenne et de la portée du cadre juridique commun de protection. L'immédiateté de ces échanges rend également l'appréhension des règles relatives aux transferts de données particulièrement contraignante pour les entreprises proposant leurs services d'automesure. Celles-ci devront en effet, en cas de transferts de données vers des pays tiers, choisir rigoureusement leurs sous-traitants. La complexité du cadre juridique relatif aux transferts, certes susceptible de limiter le développement à grande échelle du *quantified-self*, va cependant permettre de garantir une certaine cohérence aux règles protectrices édictées. En effet, les données d'un individu seront en permanence soumises à un régime de protection équivalent, peu importe les différents transferts réalisés.

464. La mise en place d'autres mécanismes. Par ailleurs, bien que le *quantified-self* n'en soit pas à l'origine, d'autres solutions ayant permis la mise en œuvre de transferts vers des pays tiers ont été adoptées, également applicables au cas de l'automesure connectée. Expressément mentionnée à l'ancien article 70 de la loi de 1978 modifiée, cette situation concernait les cas où le traitement garantissait « un niveau de protection suffisant de la vie privée ainsi que des libertés et droits

fondamentaux des personnes », et ce grâce à deux mécanismes, qu'il s'agisse des « clauses contractuelles ou règles internes » dont il faisait l'objet. La directive de 1995 ne mentionnait que le cas des « clauses contractuelles appropriées », mais les deux solutions expressément mentionnées par la loi de 1978, qui reposaient sur une responsabilisation des responsables de traitement, ont eu vocation à être reprises et développées par le Règlement général européen.

465. Les clauses contractuelles. Les clauses contractuelles, tout d'abord, visent à permettre l'encadrement des transferts de données à caractère personnel en dehors de l'Union, en mettant en œuvre des garanties efficaces entre la société qui exporte des données et celles qui importe des données. Le but est donc de contractualiser les règles adéquates de protection des données personnels entre les différents opérateurs appelés à s'échanger des données à caractère personnel. Des modèles de clauses contractuelles types pouvaient ainsi être adoptées par la Commission européenne, sur le fondement de l'article 26, 4° de la directive de 1995 et ceux-ci pouvaient ainsi concerner non seulement les transferts entre responsables de traitement[892] mais également les transferts entre responsable de traitement et sous-traitant[893]. Ces documents faisaient notamment référence à « la limitation des transferts à une finalité spécifique » ou encore à la « qualité et proportionnalité des données ». La question des données sensibles, effectivement susceptibles d'être collectées dans le cadre du quantified-self, faisait l'objet de dispositions particulières au sein de ces documents. Celles-ci nécessitaient en effet « des mesures de sécurité appropriées » impliquant de « procéder à un cryptage approfondi pour la transmission » ou bien de « répertorier l'accès » à de telles données. L'article 46 du Règlement général précise désormais, à propos des transferts moyennant des garanties appropriées, que celles-ci peuvent être fournies par le biais de clauses contractuelles.

Permettant ainsi de procéder à un transfert de données personnelles vers un Etats tiers sans avoir à rechercher de fondement légal autorisant le transfert, les

[892] Décision de la Commission des communautés européennes n°2001/497/CE du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE [notifiée sous le numéro C(2001) 1539].
[893] Décision de la Commission du 27 décembre 2004 modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers [notifiée sous le numéro C(2004) 5271].

clauses contractuelles ne sont pourtant pas le seul mécanisme pouvant être mis en œuvre pour y parvenir. A ce titre, les règles internes d'entreprise ou *binding corporate rules* permettent d'encadrer les transferts internationaux de données au sein d'un même groupe de sociétés. A l'origine absentes de la directive de 1995, celles-ci ont été consacrées par le RGPD en son article 47 qui précise que ces règles, qui doivent nécessairement être juridiquement contraignantes, sont « mises en application par toutes les entités concernées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjoint ». Ainsi limitées aux transferts au sein d'un groupe de sociétés, ces règles visent à garantir un certain niveau de protection lorsque des transferts internationaux ont lieu au sein d'un même groupe.

466. Un mécanisme limité aux groupes d'entreprises. Le champ d'application de ces règles est en principe limité aux groupes d'entreprises, mais cette notion semble pouvoir être entendue largement. Le groupe de l'article 29 y a ainsi juxtaposé les termes de « filiales » et de « multinationales », pour « décrire une situation dans laquelle les règles de gestion des données à caractère personnel seraient rendues homogènes au sein du groupe par la volonté du siège »[894]. Cette référence à la notion de contrôle est également reprise par le Règlement européen qui distingue d'un côté l'entreprise ayant le contrôle et d'autre part, l'entreprise étant contrôlée[895]. Cette solution semble pouvoir trouver un écho particulier en matière d'automesure connectée. Il n'est en effet pas rare qu'une multinationale opérant dans le secteur du numérique fasse l'acquisition de filiales spécialisées dans un domaine particulier. Les *BCR* permettent alors d'encadrer les transferts ayant lieu entre les différentes entreprises, lorsque ceux-ci se font vers des Etats tiers.

467. Les autres mesures. Le Règlement européen semble donc de prime abord favoriser les solutions fondées sur les clauses contractuelles ou sur les règles internes d'entreprise. Mais il mentionne également à l'article 46, relatif aux « transferts moyennant des garanties appropriées », donc ceux qui ne sont pas fondés sur une

[894] Sabine Marcellin, Jérôme Semik, « La responsabilité des traitements de données partagés dans un groupe », *Dalloz IP/IT*, 2017, p. 632.
[895] Le considérant 37 du Règlement indique ainsi qu'un « groupe d'entreprises devrait couvrir une entreprise qui exerce le contrôle et ses entreprises contrôlées, la première devant être celle qui peut exercer une influence dominante sur les autres entreprises du fait, par exemple, de la détention du capital, d'une participation financière ou des règles qui la régissent, ou du pouvoir de faire appliquer les règles relatives à la protection des données à caractère personnel ».

décision d'adéquation de la part de la commission, une liste de mesures permettant de procéder à des transferts de données. Ces garanties appropriées, susceptibles d'être fournies « sans que cela ne nécessite une autorisation particulière de la part d'une autorité de contrôle » peuvent par exemple et pour n'en citer que deux, reposer sur l'adoption de codes de conduite ou de mécanismes de certification sur les fondements des articles 40 et 42 du Règlement.

L'ancien article 69 de la loi Informatique et Libertés précisait auparavant les autres modalités selon lesquelles il pouvait être procédé à un transfert de données à caractère personnel vers un pays n'appartenant pas à la Communauté européenne n'assurant pas un niveau de protection suffisant. Parmi ces conditions, on retrouvait notamment celle de consentement exprès donné par l'individu. D'autres possibilités de transferts étaient ensuite prévues, notamment fondées par exemple sur « l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesure précontractuelles prises à la demande de celui-ci » ou sur la conclusion ou « l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers ». Ces dispositions sont reprises et largement complétées par le RGPD qui intègre en son article 49 ces « dérogations pour des situations particulières ». La loi Informatique et Libertés réécrite présente également, à l'article 113, les exceptions permettant la mise en œuvre de tels transferts, également applicables à l'automesure connectée et aux transferts ayant vocation à être mis en œuvre dans ce cadre. Ces différentes mesures, en contribuant à renforcer la protection des données transférées, permettent aujourd'hui un encadrement satisfaisant des transferts. Pourtant, la question particulière des transferts opérés vers les Etats-Unis est laissée en suspens.

B. L'encadrement particulier des transferts outre-Atlantique

468. Les Etats-Unis représentent, à différents égards, un cas particulier en matière d'innovation et de réglementation applicable à la protection des données personnelles. Historiquement d'abord, cette nation apparaît comme le principal incubateur de nouvelles technologies, concentré majoritairement en Californie au sein de la Silicon Valley (*Apple*, *Google*, *Facebook* ou encore *Fitbit* y ont leur siège

social). Cette concentration, à la fois technique et économique, fait des Etats-Unis un acteur majeur du déploiement de solutions fondées sur le traitement et l'échange de données personnelles. Juridiquement ensuite, la culture protectrice des données personnelles telle qu'elle est mise en œuvre et standardisée en Europe ne trouve pas d'équivalence outre-Atlantique.

Le Ier amendement, intégré au *Bill of Rights*, marque d'abord une opposition conceptuelle forte entre la liberté d'expression consacrée par le texte et le développement d'une législation protectrice de la vie privée, fondement même de la protection des données personnelles[896]. Des divergences existent ensuite sur la notion même de donnée à caractère personnel. Le concept européen est certes très large mais la notion de *Personally Identifiable Information* utilisée par la législation américaine se montre beaucoup plus restrictive et est parfois uniquement envisagée de façon sectorielle, en fonction des différentes branches d'activités (banques, santé, administrations)[897]. Ces divergences ont dès lors progressivement entraîné une remise en question du mécanisme de confiance existant entre Union européenne et Etats-Unis **(1)**, bien que celui-ci fasse actuellement l'objet d'un certain renouveau **(2)**.

1. Une confiance remise en question

469. Les Etats-Unis ont cherché à rester « fidèles à un principe d'intervention minimum en matière économique » même si son administration fédérale a « assez rapidement pris conscience que le régime mis en place au niveau européen entraînait des restrictions significatives aux transferts d'informations entre les Etats-Unis et l'Union européenne »[898]. Plusieurs éléments permettent d'illustrer ces restrictions. Celles-ci sont d'abord fondées sur les différences de régime existant et sont notamment matérialisées par le fait que la protection de la vie privée, telle que mentionnée par le IVème amendement, est effective uniquement à l'égard du gouvernement. La protection à l'égard d'acteurs privés, reconnue au niveau de la

[896] Jeffrey Rosen, « The right to be forgotten », *Stanford Law Review*, Online, 64, 2011, p. 88.
[897] Gregory Voss, « Le concept de données à caractère personnel : divergences transatlantiques Safe Harbor et Privacy Shield », *Dalloz IP/IT*, 2016, p. 119.
[898] Elisabeth Quillatre, Jean-Baptiste Thomas Sertillanges, « Libre circulation des données à caractère personnel au sein du marché intérieur et de l'espace de liberté sécurité justice : vers une diversification des instruments de régulation », *Les Petites affiches*, 3 février 2011, n° 24, page 3.

Common Law de chaque Etat, est également assurée par des lois fédérales applicables à plusieurs secteurs de l'industrie. Enfin, la protection des données personnelles est assurée sur le fondement de l'interdiction de toute pratique déloyale dans le commerce, sous le contrôle de la *Federal Trade Commission*, agence chargée de l'application du droit de la consommation.

470. Pour répondre aux interrogations suscitées par ce cadre juridique fragmenté, un système de protection a été développé en collaboration entre le ministère du Commerce des Etats-Unis et la Commission européenne, dans le but de permettre la poursuite des transferts de données. Des discussions ont été entamées dès 1998 mais le mécanisme du *Safe Harbor* n'a été véritablement opérationnel qu'à partir du 26 juillet 2000 avec l'adoption d'une décision 520/2000/CE de la Commission européenne qui a fixé un ensemble de règles garantissant un niveau suffisant de protection des données personnelles par les entreprises et administrations situées aux Etats-Unis. Visant à reconnaître le caractère adéquat des règles de protection utilisées outre-Atlantique, le *Safe Harbor* révèle sa spécificité grâce au mécanisme de certification volontaire qu'il met en œuvre.

Ainsi, le procédé relatif à cette certification repose sur une démarche volontaire de l'entreprise souhaitant adhérer aux principes contenus dans l'accord. Cette certification s'effectue concrètement par une notification au Ministère du commerce américain qui enregistre la demande et publie la liste des entreprises certifiées. Si la certification est volontaire, « l'engagement de respecter le dispositif du *Safe Harbor* est contraignant pour les entreprises adhérentes qui acceptent en se certifiant d'être contrôlées par les autorités publiques »[899]. La *Federal Trade Commission* peut donc sanctionner sur le fondement des pratiques commerciales déloyales les entreprises qui ne respectent pas le niveau de protection mis en oeuvre[900]. Le système de protection, permettant le transfert de données personnelles depuis l'Union européenne vers les Etats-Unis repose sur la prise en compte d'un certain nombre de documents regroupant d'une part une liste de principes (parmi lesquels on peut retenir le droit à l'information, le droit d'accès ou encore la sécurité

[899] Anne Debet, Jean Massot, Nathalie Metallinos, *op. cit.*, p. 680.

des données), une série de « questions fréquemment posées » d'autre part, et enfin, des échanges de courriers entre le Ministère américain du commerce, la *FTC* et la Commission européenne.

471. Malgré une certaine opposition du Parlement européen lors de la mise en place du mécanisme d'adéquation[901], le *Safe Harbor* semble avoir permis, au moins dans un premier temps, le développement du *quantified-self* et la pérennité des échanges de données réalisés grâce aux objets connectés. La liste des entreprises adhérentes au mécanisme de certification révèle ainsi que de nombreuses sociétés opérant dans le domaine de l'automesure connectée (telles que Garmin, Fitbit, Apple, Nike, Google ou encore Microsoft) ont adhéré aux règles de protection mises en œuvre afin de permettre le transfert de données entre les continents européens et américains.

Le *Safe Harbor*, après avoir fait l'objet de différentes évaluations[902], a pourtant été progressivement remis en question, notamment à la suite des révélations d'Edward Snowden en 2013 sur le programme de surveillance *Prism* de la *National Security Agency* (NSA)[903]. Dans ce climat de méfiance, une plainte rejetée devant l'autorité de contrôle irlandaise et considérant que « le droit et les pratiques des États-Unis n'offraient pas de protection suffisante contre la surveillance, par les autorités publiques, des données transférées vers ce pays »[904] a fait l'objet d'un appel devant la *High Court of Ireland*, cette dernière ayant en fin de compte saisi la Cour de Justice de l'Union européenne[905]. L'autorité irlandaise de protection a rejeté la plainte, au motif notamment que, dans sa décision du 26 juillet 2000, la Commission considérait

---

[900] Carole Moal-Nuyts, « Le transfert de données à caractère personnel vers les Etats-Unis conformément au droit européen », *RTD eur*., 2002, p. 451.
[901] Résolution du Parlement européen sur le projet de décision de la Commission relative à la pertinence des niveaux de protection fournis par les principes de la sphère de sécurité et les questions souvent posées y afférentes, publiées par le ministère du Commerce des Etats-Unis », doc. n° A5-0177/2000.
[902] Voir notamment : Commission européenne, L'application de la décision de la Commission 520/2000/CE du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiées par le ministère du commerce des Etats-Unis d'Amérique, SEC (2002) 196, 13 décembre 2002.
[903] Nathalie Laneret, Solène Hamon, « Quel avenir pour les transferts internationaux ? », *Dalloz IP/IT*, 2018, p. 31.
[904] La plainte en question, relative à l'utilisation du réseau social Facebook par un citoyen autrichien, portait à l'origine sur la question du transfert des données de l'individu concerné de la filiale irlandaise du réseau social à des serveurs situés sur le territoire des Etats-Unis.
[905] Cécile Théard-Jallu, Jean-Marie Job, Simon Mintz, « Invalidation de l'accord Safe Harbor par la CJUE : portée, impacts et premiers éléments de solution », *Dalloz IP/IT*, 2016, p. 26.

que les Etats-Unis assuraient « un niveau adéquat de protection aux données à caractère personnel transférées dans le cadre du régime dit de la sphère de sécurité. La Haute Cour de justice irlandaise a pourtant souhaité savoir si cette décision de la Commission avait pour effet d'empêcher une autorité nationale de contrôle d'enquêter sur une plainte alléguant qu'un pays tiers n'assurait pas un niveau de protection adéquat et, le cas échéant, « de suspendre le transfert de données contesté »[906].

La Cour a d'abord considéré qu'aucune disposition de la directive ne permettait d'empêcher les autorités nationales de contrôler les transferts de données personnelles vers des pays tiers ayant fait l'objet d'une décision de la Commission. La juridiction européenne s'est également prononcée sur la validité de la décision de la Commission du 26 juillet 2000 instituant le mécanisme du *Safe Harbor*. A ce titre, l'arrêt de grande chambre du 6 octobre 2015[907] en arrive à la conclusion que les États-Unis n'assurent pas un niveau de protection équivalent, et donc adéquat, avec pour conséquence l'invalidation de la décision 2000/520. Fondée notamment sur le fait qu'une « réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte »[908], l'arrêt de la Cour marque la disparition rétroactive du Safe Harbor, conformément à la jurisprudence européenne considérant qu'un « arrêt de la Cour constatant à titre préjudiciel l'invalidité d' un acte communautaire a, en principe, un effet rétroactif »[909]. L'arrêt de la Cour a eu pour conséquence de retirer tout fondement légal aux transferts qui étaient jusque-là réalisés et a obligé, par la même occasion, le recours à des solutions alternatives permettant la poursuite de ces échanges[910]. Un nouvel accord a par la suite été discuté

[906] Cour de justice de l'Union européenne, « La Cour déclare invalide la décision de la Commission constatant que les États-Unis assurent un niveau de protection adéquat aux données à caractère personnel transférées », Communiqué de presse n°117/15.
[907] CJUE, 6 oct. 2015, aff. C-362/14, *M. Schrems c/ Data Protection Commissioner*.
[908] *Ibid*.
[909] CJCE, 26 avr. 1994, aff. C-228/92, *Roquette Frères*.
[910] Céline Castets-Renard, « Invalidation du Safe Harbor par la CJUE : tempête sur la protection des données personnelles aux États-Unis », *Recueil Dalloz*, 2016, p. 88.

et mis en place, à l'appel du G29 notamment, celui-ci permettant, dans une certaine mesure, le renouvellement de la confiance entre Europe et Etats-Unis[911].

2. Une confiance partiellement renouvelée

472. La conclusion d'un nouvel accord. Dépourvus de fondement légal depuis l'annulation rétroactive du *Safe Harbor* par la Cour de justice de l'Union, les transferts de données vers les Etats-Unis ont semblé un temps compromis. Des solutions transitoires reposant sur les mécanismes alternatifs de la directive ont dû être mis en place et le groupe de l'article 29 s'est réuni dès le 15 octobre 2015 pour procéder à l'analyse des conséquences de la décision de la Cour de justice. Une position commune sur la question a été adoptée[912] et un ultimatum a été exprimé quant à la mise en œuvre d'un nouvel accord visant à assurer la poursuite des transferts de données vers les Etats-Unis. L'appel lancé par le groupe de l'article 29 aux autorités européennes et américaines a permis de mener à la conclusion, début 2016, d'un nouvel accord visant à réglementer ces transferts.

Intitulé *Privacy Shield* ou « bouclier de protection de la vie privée », le nouvel accord adopté et entré en vigueur depuis le 1er août 2016 reprend le même mécanisme d'auto-certification précédemment à l'œuvre, tout en le renforçant, notamment à l'égard de l'accès aux données par le gouvernement américain. Les États-Unis ont par exemple donné des garanties écrites sur le fait que l'accès aux données personnelles par les autorités publiques pour des motifs d'application de la loi et de sécurité nationale feraient l'objet de limitations claires, de garde-fous et de mécanismes de surveillance[913]. Ces exceptions fondées sur un critère de nécessité et de proportionnalité doivent permettre d'éviter l'hypothèse d'une surveillance massive des données transférées par les autorités, comme c'était notamment le cas avec le programme *PRISM*.

473. Le renforcement des garanties. La décision d'adéquation du *Privacy Shield* rendue par la Commission européenne le 12 juillet 2016 renforce les garanties

[911] Bernard Haftel, « Transferts transatlantiques de données personnelles : la Cour de justice invalide le Safe Harbour et consacre un principe de défiance mutuelle », *Recueil Dalloz*, 2016, p. 111.
[912] Statement of the Article 29 Working Party, Brussels, 16 october 2015.

entourant les transferts de données personnelles vers les Etats-Unis, notamment concernant l'obligation d'information des individus qui s'applique aux données collectées, aux finalités, à l'existence d'un droit d'accès ou encore à l'existence d'un organe indépendant de résolution de litiges[914]. Les solutions protectrices des données en amont du transfert sont renforcées et les individus disposent également désormais de recours effectifs permettant de faire valoir leurs droits, notamment par le biais d'un recours à un mécanisme de médiation[915]. Par ailleurs, les sanctions mises en œuvre, parmi lesquelles une éventuelle « radiation de la liste des entreprises adhérant au dispositif », ont eu vocation à renforcer les garanties apportées aux individus[916].

474. Les limites. Pourtant, malgré ce renforcement des garanties, le *Privacy Shield* souffre déjà de certaines incertitudes concernant l'effectivité des mécanismes protecteurs mis en œuvre, à l'image des critiques formulées à l'encontre du *Safe Harbor* par les institutions européennes avant même son invalidation par la Cour de justice. Décrié avant même son adoption[917], le *Privacy Shield* présenterait encore selon le G29 des lacunes concernant l'indépendance du médiateur chargé de résoudre les litiges et concernant les limitations apportées aux cas de surveillance massive[918]. Surtout, il serait susceptible de créer un déséquilibre concurrentiel à l'égard des entreprises européennes en raison des obligations moindres pesant sur celles situées aux Etats-Unis. Enfin, certains droits désormais consacrés par le nouveau Règlement général, tel que le droit à l'effacement des données en lien avec la finalité, sont absents du dispositif[919]. Le niveau d'adéquation mis en œuvre, limité selon la Commission européenne[920], serait dès lors plus susceptible de se rapprocher des exigences de la directive de 1995 que de celles du nouveau Règlement européen. Or, ces limites sont susceptibles d'impacter directement les mécanismes de *quantified-*

---

[913] Céline Castets-Renard, « Le Privacy Shield », *Dalloz IP/IT*, 2016, p. 113.
[914] Céline Castets-Renard, « L'adoption du Privacy Shield sur le transfert de données personnelles », *Recueil Dalloz*, 2016, p. 1696.
[915] Laura Sadoun-Jarin, « La Commission européenne a adopté le bouclier de protection des données transatlantiques », *Dalloz Actualité*, 29 juillet 2016.
[916] Éléonore Scaramozzino, « Adoption du bouclier de protection des données UE-EU », *JAC 2016*, n°38, p.10.
[917] Commissaire européen à la protection des données, Avis concernant le « Bouclier vie privée UE-États-Unis », Avis 4/2016, 30 mai 2016, p. 3.
[918] Groupe de l'article 29, Avis WP 238 sur le projet de décision d'adéquation du *Privacy Shield*, 13 avril 2016
[919] Céline Castets-Renard, « Adoption du Privacy Shield : des raisons de douter de la solidité de cet accord », *Dalloz IP/IT*, 2016, p. 444.

self, en raison notamment du recours de plus en plus fréquent aux solutions de *cloud-computing* qui se sont généralisées ces dernières années.

§2. Le recours à l'informatique en nuage

475. Les problématiques relatives aux accords entourant les transferts hors de l'Union européenne mobilisent aujourd'hui l'attention. En effet, « la technologie informatique qui est le principal levier du marché repose précisément sur le transfert de données, quelque part dans le monde, à l'appui d'un contrat entre un prestataire informatique et son client »[921]. Or, ces transferts de données sont caractéristiques de l'informatique en nuage et du *cloud-computing*. Bien que les définitions qui en sont données ne sont pas forcément unifiées, il est possible d'en retenir deux. La première, donnée par le *National Institute of Standards and Technology* (NIST), agence du Département du Commerce des Etats-Unis, indique que le *cloud* est « l'accès via un réseau de télécommunications, à la demande et en libre-service, à des ressources informatiques partagées configurables ». La seconde, proposée la Commission de terminologie et de néologie française, indique qu'il s'agit d'un « mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire », et qui constitue dès lors « une forme particulière de gérance de l'informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients »[922]. En d'autres termes, l'informatique en nuage met en place un stockage externalisé des données **(A)**, ces dernières pouvant également et dans certains cas faire l'objet d'une centralisation **(B)**.

A. Un stockage externalisé

476. Le recours au *cloud* computing peut avoir pour effet de brouiller les pistes quant à la destination finale des données traitées, la mondialisation du stockage des

[920] European Commission, Report from the commission to the european parliament and the council on the first annual review of the functioning of the EU-US Privacy Shield, COM (2017) 611 final, Brussels, 18.10.2017.
[921] Caroline Zorn, « Contrats de Cloud computing et données personnelles : éléments de rénovation des techniques contractuelles », *Dalloz IP/IT*, 2016, p. 453.
[922] JORF n°0129 du 6 juin 2010, page 10453, texte n° 42.

données ayant en effet tendance à complexifier l'application des règles de protection en vigueur. La généralisation du recours à l'informatique en nuage, technique virtuelle de gestion des informations, marque ainsi le passage d'une gestion interne aux instruments utilisés pour procéder à la collecte et au traitement de données, à une gestion externe qui fait intervenir d'autres prestataires. Le recours au *cloud computing* semble dès lors entraîner une perte de maîtrise de ses données pour l'individu **(1)** tout en soulevant la question de la qualification juridique du prestataire d'un tel service **(2)**.

1. Une perte de maîtrise apparente des données traitées

478. L'absence de transparence des services. Comme le relève la CNIL, « il est constaté que les clients souffrent d'une insuffisance de transparence de la part des prestataires de *cloud* quant aux conditions de réalisation des prestations, notamment sur la sécurité et sur la question de savoir si leurs données sont transférées à l'étranger, et plus précisément à destination de quels pays »[923]. Ainsi, un utilisateur du *cloud* fait face, concernant la localisation de ses données personnelles, à certaines incertitudes. Celles-ci naissent du fait que « l'utilisation du matériel est optimisée de façon dynamique à travers un réseau d'ordinateurs si bien que la localisation exacte des données ou des processus ainsi que l'information relative à l'élément de matériel qui sert effectivement à un utilisateur particulier à un moment donné ne doivent pas, en principe, concerner l'utilisateur même si cela peut avoir une incidence majeure sur le cadre juridique applicable »[924]. Dès lors, les données stockées peuvent être appelées à être retransférées, en fonction de l'espace de stockage disponible sur les différents serveurs d'un prestataire, participant à la création d'un mouvement continu de données, sans que la personne concernée par le traitement en soit forcément consciente.

Certains risques sont révélés par le recours au *cloud computing* et ils relèvent notamment d'une « absence de contrôle sur les données à caractère personnel et à une

[923] CNIL, *Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing*, 25 juin 2012, p. 1.

information insuffisante sur le mode et le lieu du traitement ou du sous-traitement des données et sur la ou les personnes qui les réalisent »[925]. Ce manque d'information dont dispose la personne concernée par le traitement, notamment sur la localisation géographique finale du stockage, est susceptible de renforcer la perte de maîtrise de l'individu sur les données stockées. En déléguant la gestion du stockage de leurs données, les clients de service de *cloud computing* sont soumis aux pratiques du prestataire, ce qui peut potentiellement les priver de la capacité à déployer les mesures techniques et organisationnelles « nécessaires pour garantir la disponibilité, l'intégrité, la confidentialité, la transparence, la séparation et la portabilité des données »[926]. La mise en œuvre de mesures protectrices effectives est ainsi rendue illusoire par cette externalisation.

479. Les transferts successifs de données. Par ailleurs, une difficulté supplémentaire est susceptible de se présenter lorsqu'un premier transfert de données à caractère personnel réalisé dans le cadre d'une prestation de *cloud computing* fait l'objet d'un éventuel transfert ultérieur. Pour les transferts successifs réalisés au sein de l'espace économique européen, la présomption de niveau de protection adéquat ou suffisant n'entraînera pas de complications. En revanche, lorsque le premier transfert est fondé sur un niveau de protection suffisant ou sur des mécanismes contractuels permettant de garantir une telle adéquation, la question du transfert ultérieur vers un autre pays tiers est susceptible d'être posée. Pour y répondre, la CNIL analyse différents cas pratiques reposant sur la problématique d'un transfert ultérieur vers un pays tiers[927] et insiste, pour chaque cas de figure, sur la nécessité de prévoir des garanties visant à protéger les données et ce à chaque niveau de la chaîne de transfert. Ainsi, le modèle contractuel du *cloud computing* soulève également des hésitations sur le rôle effectif confié au prestataire et en fonction duquel le degré d'obligations à sa charge est susceptible de varier.

---

[924] Commission européenne, Communication de la commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, *Exploiter le potentiel de l'informatique en nuage en Europe*, Bruxelles, le 27 septembre 2012, COM (2012) 529 final, p. 3.
[925] G29, Avis 05/2012 sur l'informatique en nuage, 01037/12/FR, WP 96, 1er juillet 2012, p. 2.
[926] *Ibid*, p. 6.
[927] CNIL, *Les transferts de données à caractère personnel hors Union européenne,* op. cit., p. 25 à 32.

Le G29 relevait dès 2012, dans son avis sur l'informatique en nuage, que le manque d'informations fournies au client lors de la conclusion d'un contrat de *cloud* empêchait ce dernier d'avoir pleinement conscience de l'existence de traitement en chaîne faisant intervenir plusieurs sous-traitants ou du fait que les données à caractère personnel étaient traitées dans plusieurs zones géographiques au sein de l'espace économique européen ou encore en dehors de celui-ci. Le groupe de l'article 29 a recommandé que de plus amples renseignements soient fournis sur les transferts ultérieurs de données, en vertu notamment des articles 13 et 14 du RGPD relatifs aux informations à fournir et à la sous-traitance. En effet, outre des questions relatives au droit applicable lorsque le lieu d'établissement d'un fournisseur de service en nuage est difficile à déterminer[928], le recours au *cloud* pose la question de la qualification juridique du prestataire.

2. Une qualification juridique complexe du prestataire

480. Les chaînes de prestataires. L'informatique en nuage pose des questions qui sont relatives à la localisation précise des données stockées. Mais l'identification des différents interlocuteurs est également complexe, notamment en raison des « chaînes de prestataires et d'intervenants divers tels que des fournisseurs d'infrastructure ou de communications »[929] qui sont déployées. La destination finale des données ainsi que la qualification juridique de chacun des intervenants semblent difficiles à déterminer. Or, l'identification des obligations de chacun lors de la mise en œuvre d'une solution de stockage externalisé dépend de ces deux éléments. Cette qualification peut se révéler délicate en raison des différents rôles que le prestataire d'un service de *cloud* peut endosser et par les relations qui peuvent s'établir entre responsable de traitement, sous-traitant et sous-traitant ultérieur. Pourtant, comme l'a indiqué le G29 avant l'entrée en vigueur du RGPD, il est « impératif d'assurer le respect des règles de protection des données et d'attribuer clairement les responsabilités en cas d'infraction à ces dispositions, afin d'éviter tout affaiblissement de la protection des données à caractère personnel, afin que toute apparition de conflits négatifs de compétence ou de hiatus, qui reviendraient à ce que

[928] Commission européenne, *op. cit.*, p. 10.

certains droits ou obligations découlant de la directive ne soient plus assumés par aucune des parties »[930].

En principe, le client de services de *cloud computing* détermine en amont la finalité du traitement. De même, c'est lui qui décide de « l'externalisation de ce traitement et de la délégation de tout ou partie des activités de traitement à une organisation externe : le client agit donc en qualité de responsable du traitement de données »[931]. Il est ainsi identifié par la réglementation comme étant l'entité sur laquelle pèse les obligations légales relatives à la mise en œuvre d'un traitement. Le fournisseur du service de *cloud* peut dès lors être considéré comme un sous-traitant, entendu au sens de la directive de 1995 et du RGPD comme « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement ». Identifiés de la sorte, chacun des intervenants dispose d'un rôle clairement établi et d'éléments de responsabilité précisément déterminés, y compris pour les cas de figure ou un sous-traitant ferait appel à un sous-traitant ultérieur[932].

L'étude des contrats auxquels il est fait recours dans le cadre de la fourniture d'un service de *cloud* révèle une certaine asymétrie entre prestataires et clients, limitant les possibilités pour les responsables de traitement des données de se « conformer aux exigences applicables en matière de traitement des données à caractère personnel dans le cadre d'un environnement d'informatique en nuage »[933]. Cette asymétrie peut conduire à une répartition inadéquate des responsabilités liées au respect de la législation sur la protection des données en raison de qualifications de responsable du traitement et de sous-traitant qui ne reflètent pas correctement le niveau de contrôle exercé sur les moyens de traitement. Le responsable de traitement, client du service d'externalisation, ne sera pas toujours à même d'exercer son

---

[929] *Ibid*.
[930] G29, Avis 05/2012, *op. cit*., p. 9.
[931] *Ibid*.
[932] Pour rappel, cette situation est précisément réglementée par l'article 28 du RGPD qui prévoit en son 4° les modalités selon lesquelles un sous-traitant peut faire appel à un sous-traitant ultérieur.
[933] Contrôleur européen de la protection des données, Avis du contrôleur européen de la protection des données relatif à la communication de la Commission intitulée « Exploiter le potentiel de l'informatique en nuage en Europe », Bruxelles, 16 novembre 2012, p. 7.

contrôle, en raison de la nature des contrats conclus, contrats d'adhésion dont les conditions générales, soustraites à la négociation, sont déterminées à l'avance par l'une des parties[934].

481. La responsabilité conjointe. L'identification de chacune des parties, rendue complexe par le recours à des contrats d'adhésion qui empêchent un contrôle effectif des moyens mis en œuvre par le prestataire de service de cloud, peut dès lors nécessiter le recours à la notion de responsable conjoint du traitement ou de coresponsable du traitement. Préconisé par la CNIL dès 2012[935], le recours à la notion de responsabilité conjointe permet d'identifier avec plus de précision l'entité interlocutrice de la personne concernée d'une part, et celle responsable vis-à-vis des autorités de protection des données personnelles d'autre part. L'article 26 du RGPD relatif aux responsables conjoints du traitement trouve donc un écho particulier en matière de *cloud computing* puisqu'il prévoit justement les cas dans lesquels « deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement ». Alors qu'un contrat relatif aux exigences de transparence doit être conclu entre les responsables conjoints, le recours à un tel mécanisme a le mérite de renforcer la lisibilité des droits et obligations de chacune des parties engagées dans la mise en œuvre d'une prestation d'informatique en nuage.

Le *cloud-computing* est aujourd'hui le moyen technique privilégié pour procéder au stockage des données informatiques. Le *quantified-self* repose également sur ce procédé de stockage, en raison du nombre important d'informations créées. La notion de responsabilité conjointe inscrite à l'article 26 du RGPD permet une protection renforcée des informations traitées. Cependant, le recours au *cloud* est également susceptible de procéder à un renforcement des risques au niveau technique.

[934] Antoine Gendreau, « La dématérialisation du dépôt : l'exemple du contrat de cloud computing », *AJ contrat*, 2016, p. 519.
[935] Celle-ci indique en page 6 de ses « Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing » que « dans de telles situations, le prestataire pourrait a priori être considéré comme conjointement responsable en vertu de la définition de « responsable du traitement » fournie à l'article 2 de la directive 95/46/CE, puisqu'il participe à la détermination des finalités et des moyens des traitements de données à caractère personnel ».

B. Une centralisation des données

482. Les données à caractère personnel stockées dans le *cloud* font face à de nouveaux risques qui reposent sur l'architecture du réseau elle-même. La soumission de ces données à un stockage externalisé par un prestataire tiers est en effet susceptible de conduire à leur regroupement au sein d'un même lieu géographique et d'un même serveur informatique. Eloignées des individus auxquels elles se rapportent et concentrées en un même lieu, ces informations sont ainsi soumises à un risque renouvelé quant à leur sécurité **(1)** nécessitant par la même occasion de repenser leurs modalités d'accès **(2)**.

1. Un risque d'atteinte à la sécurité des données

483. L'éclatement du stockage. La question de la localisation des serveurs de données sur lesquels sont stockées des données à caractère personnel est primordiale en matière de *cloud computing* : la répartition des données à laquelle il est procédé pour la mise en œuvre de ces différents services apparaît être un facteur de vulnérabilité pour les données traitées[936]. En effet, cet externalisation du stockage, qui conduit parfois à l'éclatement des données, est susceptible de constituer « un facteur d'aggravation des risques d'atteinte à la confidentialité des données »[937]. Cette affirmation concerne non seulement l'éclatement juridique de la protection entre différentes législations mais elle peut également s'appliquer au risque technique encouru, fondé sur un éclatement géographique des informations traitées. En effet, les données stockées grâce à une solution d'informatique en nuage sont amenées à faire l'objet de nombreux transferts entre différents serveurs informatiques, en fonction de la place disponible sur chacun d'eux ou de l'évolution de la relation contractuelle entre prestataire et client. Un prestataire de *cloud* peut décider de stocker les données sur un premier serveur avant de les déplacer ensuite si celui-ci présente des limites quant à ses capacités de stockage. Le prestataire de *cloud* peut ainsi optimiser l'espace de stockage dont il dispose, mais il soumet dès lors les données à un risque

[936] Caroline Zorn, « Contrats de Cloud computing et données personnelles : éléments de rénovation des techniques contractuelles », *Dalloz IP/IT*, 2016, p. 453.
[937] ANSSI, *Maîtriser les risques de l'infogérance : externalisation des systèmes d'information*, décembre 2010, p. 8.

de détournement supplémentaire en les faisant transiter entre différents supports de stockage.

484. Le respect de référentiels pour une sécurité renforcée. La chaîne de traitement des données mise en œuvre par les différentes externalisations réalisées multiplie les risques d'atteintes aux données personnelles. Evidemment concernés par les dispositifs légaux relatifs à la sécurité des données, les mécanismes de stockage du *cloud* font également l'objet de nombreuses recommandations visant à garantir un niveau de sécurité renforcé des infrastructures utilisées. Outre la conformité à certaines normes internationales, notamment ISO 27001 et ISO/IEC 27018, « premier standard applicable aux prestataires de *cloud* pour la protection des données »[938], CNIL, G29 et CEPD se sont prononcées et se prononcent tous pour la mise en œuvre de mesures de sécurité renforcées, passant notamment par le recours à une analyse des risques[939], telle qu'elle est également préconisée par l'article 32 du RGPD. La structure particulière du *cloud* nécessite à ce titre une attention particulière sur l'ensemble de la chaîne de traitement mise en œuvre en ce qu'une défaillance de sécurité en un endroit de la chaîne est susceptible de compromettre l'ensemble du dispositif[940]. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a développé un référentiel dit EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) permettant à ce titre d'étudier les risques inhérents au déploiement d'un système d'information.

485. La centralisation des données. Par ailleurs, si les données semblent être parfois éclatées, elles peuvent à l'inverse être centralisées par l'opérateur en charge du stockage. Un autre risque est ici susceptible d'apparaître, les données d'un individu provenant parfois de sources différentes et soumises à un stockage externalisé étant toutes centralisées en un même lieu géographique et au sein d'un même *data center*. Dans cette hypothèse, la vulnérabilité du dispositif repose sur la centralisation en un même lieu des données traitées, accroissant ainsi le risque de

[938] Marc Mossé, « Quand le Cloud rime avec cybersécurité », *Dalloz IP/IT*, 2016, p. 16.
[939] Voir par exemple la recommandation n°3 formulée par la CNIL dans ses recommandations de 2012 ou le point n°90 de l'avis du Contrôleur européen qui recommandent tous deux de procéder à une évaluation des risques.
[940] Il est possible de citer, à titre d'exemple, l'attaque informatique subie par le cabinet Deloitte par laquelle des individus ont accédé à des documents stockés sur le *cloud* de l'entreprise et auquel ils ont eu accès en utilisant l'identifiant et le mot de passe d'un compte administrateur.

perte de maîtrise informationnelle et ajoutant un niveau de complexité supplémentaire à la question de la gouvernance des données à caractère personnel. Ce cas de figure est d'autant plus susceptible de se produire dans le cadre de la pratique de l'automesure. Les informations collectées, provenant de différentes sources, n'ont à l'origine pas vocation à être croisées mais celles-ci peuvent, avec le *cloud computing*, être agrégées par une seule et même entité, qu'il s'agisse du fournisseur de service ou d'un tiers spécialisé dans le stockage.

Les conséquences d'une telle centralisation sont potentiellement néfastes pour l'individu puisqu'elles permettent de mettre à la disposition d'une seule entité des données concernant un même individu et qui n'ont en théorie pas vocation à être recoupées[941]. Un premier risque, relatif à la sécurité informatique, est ainsi susceptible de se manifester. En regroupant des données relatives à une même personne au sein d'un même serveur informatique, les cas d'accès non autorisés sont susceptibles de permettre une interconnexion d'informations différentes permettant de définir un profil de l'individu, hypothèse difficilement envisageable lorsque les données sont fragmentées entre différents lieux de stockage. Par ailleurs, cette hypothèse pose la question de la confidentialité des données confiées à l'opérateur du service d'informatique en nuage.

Lorsqu'un individu utilise plusieurs dispositifs de *quantified-self* (balance connectée et podomètre par exemple) et que ces différents services ont recours au même prestataire de *cloud computing*, la question de la séparation entre ces données issues de sources différentes est susceptible de se poser. L'objectif final de l'automesure repose sur le croisement exponentiel de données en vue d'obtenir une information qui soit la plus précise possible. Mais il faut éviter que des informations, stockées au même endroit par le même prestataire, puissent être croisées sans que la personne concernée ne soit avertie. Les modalités d'accès aux données stockées doivent donc être déterminées clairement, afin de contenir les éventuels risques liés à l'utilisation massive du *cloud*. Cette problématique est d'autant plus importante que la complexité des solutions mises en œuvre est susceptible d'empêcher la personne

[941] Primavera De Filippi, Smari McCarthy, « Cloud computing centralization and data sovereignty », *European Journal of Law & Technology*, Vol. 3, No 2, 2012.

concernée par le traitement d'avoir pleinement conscience des enjeux relatifs à un tel accès. Dès lors, apparaît la nécessité de repenser ces modalités d'accès relatives aux données stockées dans le *cloud*.

2. Des modalités d'accès à repenser

486. Les différents modèles de services. Les solutions d'informatique en nuage, malgré une appellation unifiée sous le terme de *cloud computing*, peuvent prendre plusieurs formes. A ce titre, le *NIST* distingue entre trois modèles de services qui peuvent chacun revêtir quatre modèles de déploiement. Le modèle dit SaaS (*software as a service*) repose sur un service offert en ligne via différentes applications par un fournisseur et qui sont mises à disposition des utilisateurs finaux. Le modèle dit PaaS (*platform as a service*) implique qu'un fournisseur mette à disposition d'utilisateurs des services de développement et d'hébergement des applications. Enfin, le modèle dit IaaS (*infrastructure as a service*) implique pour l'utilisateur de disposer d'une infrastructure directement située chez son fournisseur de service. Pour chacun de ces différents services, les moyens déployés peuvent l'être dans un environnement qui repose sur un nuage public, privé internalisé, externalisé ou hybride. Dans un *cloud* privé internalisé, un seul client dispose de la faculté d'utiliser le service alors que dans un *cloud* privé externalisé, la plateforme est dédiée à plusieurs utilisateurs sélectionnés. Enfin, si le *cloud* public est accessible à tous et qu'il met en œuvre un partage des ressources entre tous les clients, le *cloud* hybride permet une « superposition entre plusieurs *clouds* privés et publics »[942].

Les différents services de *cloud* qui sont mis en œuvre pose la question des modalités d'accès aux données stockées, qu'il s'agisse de celles des clients eux-mêmes, des fournisseurs de moyens de stockage externalisés ou des tiers éventuels. Comme l'a souligné le G29 dans un avis du 1er juillet 2012, « dans les infrastructures en nuage, les ressources telles que le stockage, la mémoire et les réseaux sont partagés entre de nombreux locataires, ce qui crée de nouveaux risques de voir les données divulguées et traitées à des fins illégitimes »[943]. Il est dès lors rappelé la

[942] Thomas Lange, « Cloud computing et données personnelles : les clauses à maîtriser », *Dalloz IP/IT*, 2016, p. 459.
[943] G29, Avis 05/2012, *op. cit.*, p. 19.

nécessité de respecter le principe de finalité, tel qu'il est mentionné dans les différents textes relatifs à la protection des données personnelles. Par ailleurs, la structure de gouvernance mise en œuvre doit garantir, selon le principe du moindre privilège, que les administrateurs et les utilisateurs n'accèdent « qu'aux informations nécessaires pour servir leurs objectifs légitimes »[944].

487. Les modalités d'accès. La structure du *cloud*, telle qu'elle est déployée dans le cadre d'un service de type *IaaS* visant simplement à permettre un stockage externalisé, n'implique qu'un rôle en théorie restreint pour le fournisseur du service. Mais l'étendue des moyens mis en œuvre dans les autres hypothèses nécessite de garantir que les accès aux données soient maîtrisés et réglementés. Surtout, dans le cadre des droits qui sont garantis aux individus, il est nécessaire que le fournisseur du service d'informatique en nuage permette au responsable du traitement d'accéder aux données qui lui ont été confiées, afin de pouvoir garantir le droit d'accès dévolu *in fine* à la personne concernée. En effet, comme l'a indiqué le G29, « un fournisseur d'informatique en nuage ne fournit pas toujours les mesures et les outils nécessaires pour permettre au responsable du traitement de gérer les données, par exemple en termes d'accès, de suppression ou de correction des données »[945].

Le droit d'accès, tel qu'il est formulé à l'article 15 du RGPD, pourrait ainsi se retrouver dilué en raison de la chaîne de traitement mise en œuvre par le recours au *cloud computing* et démultipliée dans le cadre de l'automesure : l'individu pourrait ne pas savoir avec précision à quel prestataire s'adresser, en raison du nombre toujours plus important de fournisseurs de services appelés à manipuler des données à caractère personnel. Or, le droit d'accès garanti à la personne concernée par un traitement de données personnelles doit également permettre la mise en œuvre du nouveau droit relatif à la portabilité des données, conformément à l'article 20 du RGPD[946]. Le fournisseur d'un service de *cloud* doit donc permettre à son client de récupérer ses données si celui-ci souhaite s'adresser à un autre fournisseur. Il semble

[944] *Ibid.*
[945] *Ibid.*
[946] Pour rappel, celui-ci dispose que « Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle ».

dès lors nécessaire que les prestataires de *cloud* aient recours à des protocoles standardisés permettant une migration plus facile des informations. Ces différentes problématiques, étroitement liées aux modalités d'externalisation géographique, ont de plus en plus tendance à être prise en compte par une expansion territoriale progressive du cadre juridique applicable.

SECTION II. UNE EXPANSION TERRITORIALE DU CADRE JURIDIQUE

488. L'absence d'un cadre international commun de protection des données, notamment entre Europe et Etats-Unis, est à même de soulever un certain nombre de questions relatives à la détermination de la loi applicable en cas de conflits entre responsable de traitement et personne concernée par le traitement. Ces problématiques font l'objet d'un renouveau certain en raison des capacités d'échange et de transfert d'informations rendues réalisable par le recours à des objets connectés aux performances techniques renforcées. L'internationalisation et la croissance exponentielle des échanges réalisés est dès lors susceptible de provoquer une dilution des droits des individus, confrontés à des systèmes légaux opposés et potentiellement contradictoires. La question des transferts de données est précisément encadrée, mais des questions restent en suspens lorsqu'un individu utilise un dispositif ou un service qui trouve directement sa source dans un pays tiers.

Susceptibles de porter atteinte aux droits des individus, notamment aux recours effectifs dont ils doivent disposer, ces questions sont aujourd'hui renforcées par le poids économique des opérateurs en question. Celui-ci peut en effet avoir un effet dissuasif pour les personnes concernées par un traitement de données. Soumises à des dispositions contractuelles qu'elles ne peuvent négocier[947], celles-ci sont également soumises à des règles de compétence territoriale susceptibles de limiter profondément l'effectivité de leurs droits. Pourtant, porté notamment par des mouvements jurisprudentiels nationaux et européens protecteurs des droits des individus, il est possible de constater le décloisonnement progressif des droits nationaux

[947] Cf., *supra*, n° 287.

(Paragraphe 1) et des moyens d'action mis à la disposition des individus concernés par des traitements de données à caractère personnel **(Paragraphe 2)**.

§1. Le décloisonnement des droits nationaux

489. L'instauration de règles protectrices des données à caractère personnel efficaces est confrontée au caractère mondial d'Internet et à une absence de frontières nettement définies. Ces éléments posent donc la question du champ d'application territorial de la règlementation, garantie nécessaire à l'effectivité des droits des individus. Déterminer avec précision la loi applicable est désormais difficile, plusieurs législations contradictoires étant susceptibles d'être mobilisées et invoquées. Ces éléments, qui semblent pouvoir constituer un frein à l'instauration de règles protectrices homogènes, sont pourtant pris en compte. En effet, les règles relatives au champ d'application territorial de la règlementation protectrices des données sont en principes strictement définies par les différents textes en vigueur **(1)** et l'adoption du RGPD a permis d'en élargir la portée afin de garantir l'effectivité des droits des individus **(2)**.

A. Le champ d'application territorial initialement défini

490. La rédaction initiale de la loi Informatique et Libertés ne proposait à l'origine aucune référence à la question du champ d'application territorial des dispositions qu'elle mettait en œuvre, à l'exception de celles relatives à l'outre-mer. L'internationalisation des moyens de traitement a pourtant rapidement nécessité l'introduction de mesures permettant de définir avec précision le champ d'application des règles mises en œuvre, leurs critères d'application ainsi que leur délimitation territoriale. La directive de 1995 avait mis en place certains critères alternatifs permettant de clarifier le régime applicable aux responsables de traitements ainsi qu'aux personnes concernées par de tels traitements. Ces critères ont été en partie repris en 2004 au sein de la loi Informatique et Libertés, à la suite de la transposition de la directive. Les critères mis en œuvre par la réglementation ont dès lors fait reposer l'application des différentes mesures sur des critères territoriaux relatifs d'abord à l'établissement du responsable de traitement **(1)**, mais également et de

manière alternative, sur les moyens employés pour la mise en œuvre dudit traitement **(2)**.

1. L'établissement du responsable de traitement

491. La directive de 1995 est intervenue pour déterminer l'étendue territoriales des règles mises en œuvre, en l'absence de précision de la part des législations nationales. Cela a permis d'éviter d'éventuels conflits de lois mais également de garantir une application cohérente des règles, au moins au niveau géographique. L'article 4 de la directive, en fixant les règles relatives au champ d'application territorial du texte, mentionnait le fait que le droit de l'Union s'appliquait, car la loi nationale des pays membres était applicable en vertu du droit international public. Mais un critère relatif à l'établissement du responsable de traitement a également été mobilisé par le droit européen. En effet, celui-ci avait surtout vocation à s'appliquer lorsque le traitement était « effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'Etat membre ». La loi Informatique et Libertés a repris ce critère relatif à l'établissement en 2004, en indiquant qu'étaient soumis à la loi les traitements de données à caractère personnel dont le responsable était établi sur le territoire français. Selon ce critère, le responsable d'un traitement qui exerçait son activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y était considéré comme établi. Un fournisseur de services de *quantified-self* ayant son siège en France était ainsi soumis au droit français, même si ses services pouvaient être utilisés dans d'autres pays.

492. La notion d'établissement. Les dispositions de la directive et de la loi modifiée en 2004 concernaient donc d'abord le traitement de données qui était effectué par un responsable de traitement établi sur le territoire français. Critère déterminant, le recours à la notion d'établissement du responsable de traitement impliquait dès lors que « ni la nationalité ou le lieu de résidence habituelle des personnes concernées, ni la localisation physique des données à caractère personnel » n'étaient pris en compte dans la détermination de la loi applicable[948]. Ainsi, seul comptait le territoire sur lequel était établi le responsable de traitement, la notion

d'établissement pouvant être retenue dès que celui-ci exerçait « une activité dans le cadre d'une installation, quelle que soit d'ailleurs sa forme juridique »[949]. Selon le considérant 19 de la directive, la notion d'établissement sur le territoire d'un Etat membre supposait « l'exercice effectif et réel d'une activité au moyen d'une installation stable », celle-ci ne pouvant être constituée, selon le groupe de l'article 29, par le recours à un serveur informatique, considéré comme une simple installation technique et non comme une installation stable. Le fait qu'un fabricant d'objets connectés d'automesure établi hors de l'Union européenne dispose d'un serveur sur le territoire français, afin de faire transiter les données, ne suffisait donc pas à caractériser l'établissement.

493. L'hypothèse de la pluralité d'établissements. Les critères d'application mis en œuvre par la directive de 1995 ne posaient en théorie pas de problème d'interprétation. Pourtant, une difficulté liée à la pluralité d'établissements au sein de l'Union européenne s'est présentée. En effet, de nombreux responsables de traitement ont été confrontés à la question de la détermination de la loi applicable, dans la mesure où ils disposaient de plusieurs établissements situés dans différents Etats membres[950]. En principe, chaque établissement était tenu de respecter les dispositions de l'Etat membre sur lequel il était situé. Mais une telle solution était différente lorsque les traitements effectués par un établissement sur le territoire d'un Etat membre l'étaient uniquement dans le cadre des activités d'un autre établissement. Dans ce cas de figure, le droit applicable était, selon l'avis du G29 en date de 2010, celui du second Etat membre. Cette solution nécessitait donc d'examiner le degré de participation de l'établissement aux activités dans le cadre desquelles des données à caractère personnel étaient traitées ainsi que la nature de telles activités. La notion de cadre des activités est dès lors apparu comme le facteur déterminant pour la définition du droit applicable[951].

---

[948] G29, Avis n° 8/2010 sur le droit applicable, 0836-02/10/FR, 16 décembre 2010, WP 179, p. 9.
[949] Romain Perray, JurisClasseur Administratif Données Personnelles, fascicule 274-10, 2014, p. 58.
[950] *Ibid.*
[951] G29, avis n°8/2010, *op. cit.*, p. 16.

494. La CNIL retenait, au niveau national, une conception extensive de la notion d'établissement. Ainsi, dans une décision de la formation restreinte en date du 3 janvier 2014 relative au moteur de recherche *Google*, celle-ci considérait que la filiale, *Google France SARL*, société française, permettait de caractériser l'établissement en France, au sens du texte de la loi de 1978[952]. En l'espèce, le moteur de recherche soutenait que « les services auxquels ont recours les utilisateurs installés sur le territoire français » étaient exclusivement fournis par l'entité américaine et que la filiale n'exerçait « aucune activité effective » dans le cadre de laquelle la maison mère traitait des données personnelles, impliquant dès lors qu'elle n'avait pas recours à des moyens de traitement sur le territoire français. La CNIL, au contraire, considérait que la filiale participait de manière effective à des activités liées aux traitements de données relatives aux utilisateurs des services. Elle relevait notamment que l'activité de publicité en ligne, figurant parmi les activités de la filiale déclarée au Registre du Commerce et des Sociétés, était indissociable du traitement des données des utilisateurs. Ainsi, « c'est à l'aune de l'importance que revêtent ces activités localisées en France » que la CNIL a pu considérer que la filiale française devait être « regardée comme un établissement au sens de l'article 5 de la loi n°78-17 du 6 janvier 1978 modifiée ».

L'exemple de l'application Nike+ Run Club, application de *running* permettant de calculer le temps et la distance parcourue et proposant des programmes d'entraînement personnalisés, peut être mentionné. Il serait possible de considérer que les services proposés par l'application sont exclusivement fournis par l'entité américaine de l'entreprise. La politique de confidentialité de l'application indique d'ailleurs précisément que pour la France, l'entité responsable du traitement dans le cadre de l'application de *running* est Nike, Inc, situé à Beaverton aux Etats-Unis. Mais cette application permet également de proposer de la publicité aux individus, relatives à des nouveaux produits ou à des événements. Selon l'interprétation donnée par la CNIL à propos du réseau social Facebook, cette activité de publicité en ligne permettrait de caractériser la notion d'établissement. Dans ce cas de figure précis, la

[952] CNIL, Délibération n°2013-420 du 3 janvier 2014 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société X.

filiale hollandaise de Nike, responsable du traitement en Europe, aurait été considérée comme caractérisant l'établissement. Mais d'autres critères, relatifs aux moyens de traitement, auraient permis de rattacher le traitement réalisé à la loi française.

2. Le critère alternatif des moyens de traitement

495. En plus du critère relatif à l'établissement du responsable de traitement, un second critère, relatif aux moyens utilisés par le responsable de traitement, a également été mis en œuvre. Celui-ci était applicable lorsque le responsable de traitement n'était pas établi sur le territoire français, mais qu'il avait simplement recourt à des moyens de traitement situés sur ce territoire. L'article 4 de la directive de 1995 mentionnait ainsi, parmi les critères relatifs au champ d'application territorial, un second cas de rattachement, lorsque le responsable du traitement n'était pas établi sur le territoire de l'Union. Dans ce cas de figure, ce dernier devait cependant avoir recourt « à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit Etat membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté ». Des bracelets connectés, *trackers* d'activité, proposés à la vente par une entreprise et utilisés pour procéder à une collecte de données permettaient ici de caractériser la notion de moyens. L'article 5 de la loi de 1978 modifiée reprenait également fidèlement ce critère d'application de la législation, relatif à localisation géographique des moyens de traitement utilisés.

496. L'interprétation de la notion. La notion de « moyens de traitement » ne faisait l'objet d'aucune définition légale[953]. Selon l'interprétation donnée par le G29, cette disposition présentait cependant « un intérêt tout particulier au regard du développement des nouvelles technologies, notamment de l'Internet, qui facilitent la collecte et le traitement de données à caractère personnel à distance »[954]. Le G29 semblait dès lors retenir une définition large de la notion de « moyens » permettant notamment d'englober « les intermédiaires humains ou techniques »[955]. Celui-ci, à propos des moteurs de recherche, considérait que ceux-ci avaient recours « à des

[953] Tout au plus, la directive de 1995 précisait à l'article 4, 1°, c, que ceux-ci pouvaient être « automatisés ou non ».
[954] G29, avis n°8/2010, *op. cit.*, p. 21.

moyens implantés sur le territoire de l'Union européenne du seul fait de l'utilisation d'ordinateurs personnels, de terminaux et de serveurs, voire même de la simple installation de cookies sur les terminaux des personnes concernées[956]. Pour reprendre l'exemple précité de l'application Nike+ Run Club, le fait que cette entreprise propose une application au téléchargement en France permettait de retenir la notion de « moyens » permettant de procéder à la collecte. Directive et loi de 1978 modifiée indiquaient par ailleurs qu'étaient exclus de cette mesure les moyens de traitement utilisés simplement « à des fins de transit ». Le responsable de traitement n'était dès lors pas soumis à la loi du territoire sur lequel il utilisait ces moyens lorsque les données, en transit sur le territoire, n'étaient pas immobilisées à des fins de traitement.

497. Un critère large. Le critère relatif aux moyens de traitement était par nature, relativement large. Son interprétation par les différentes autorités de protection lui a conféré un spectre encore plus important et le G29, dans un avis sur le droit applicable, a fait référence au critère du ciblage pour préciser sa portée. La référence au ciblage constituait un facteur de rattachement plus précis susceptible de compléter les critères liés aux moyens. Entendu comme « l'approche axée sur le service », ce critère faisait référence au fait que le traitement devait « cibler des personnes résidant dans l'UE pour entraîner l'application du droit de l'UE en matière de protection des données »[957]. Ce recours à la notion de ciblage limitait certaines conséquences de l'application du critère des moyens de traitement et évitait ainsi l'application du droit de l'Union a des traitements présentant un lien simplement limité avec son territoire. Lorsqu'un responsable de traitement établi hors de France avait recourt à des moyens de traitement en France pour traiter des données de non-résidents français, l'interprétation littérale du texte commandait d'appliquer la loi[958],

[955] *Ibid.*, p. 23.
[956] Romain Perray, *op. cit.*, p. 61.
[957] G29 avis n°8/2010, *op. cit.*, p. 36.
[958] Prudence Cadio, Thomas Livenais, « Photographie du champ territorial du règlement données personnelles : de nouveaux opérateurs concernés ? », *Dalloz IP/IT*, 2016, p. 347.

raison pour laquelle la CNIL avait adopté une dispense de déclaration pour ce type de situations[959].

La CNIL avait également fait référence à la notion de moyen de traitement dans sa délibération du 3 janvier 2014 précitée. Se fondant notamment sur le considérant 18 de la directive[960], celle-ci considérait qu'un *cookie* ou fichier texte ne constituait pas, en lui-même, un traitement. Cependant, elle constatait que lecture et l'écriture d'informations sur le navigateur installé sur le terminal de l'utilisateur s'effectuaient « par l'intermédiaire de *cookies*, dans le but de collecter des informations » dont la société était l'unique destinataire. Dès lors, faisant référence à l'article 2 de la loi Informatique et Libertés relatif à la qualification de traitement de données à caractère personnel, celle-ci considérait que « l'accès aux informations relatives à l'utilisateur par le vecteur du cookie et leur lecture » constituaient bien des traitements au sens de cet article. L'autorité de protection française soutenait dès lors que « l'ensemble des équipements et logiciels participant à ces actions d'écriture ou de lecture – y compris les cookies et les outils similaires » devaient être considérés comme des moyens de traitement. Cette interprétation extensive retenue par la CNIL s'insérait dans un mouvement globalisé d'élargissement du champ d'application territorial des règles en vigueur de protection des données à caractère personnel, mouvement toujours à l'œuvre actuellement.

B. Un champ d'application territorial désormais élargi

498. Les critères mis en œuvre par la directive et transposés en 2004 au sein de la loi Informatique et Libertés avaient vocation à couvrir un spectre important de situations. Mais ceux-ci ont nécessité de faire l'objet d'une certaine interprétation afin de couvrir au mieux les cas de figure susceptibles de se présenter dans le cadre de l'internationalisation grandissante des capacités de collecte et de traitement des

[959] CNIL, Délibération n° 2011-023 du 20 janvier 2011 dispensant des traitements automatisés effectués sur le territoire français par des prestataires agissant pour le compte de responsables de traitement établis hors de l'Union européenne et concernant des données personnelles collectées hors de l'Union européenne.
[960] « considérant que l'établissement, dans un pays tiers, du responsable du traitement de données ne doit pas faire obstacle à la protection des personnes prévue par la présente directive; que, dans ce cas, il convient de soumettre les traitements de données effectués à la loi de l'État membre dans lequel des moyens utilisés pour le traitement de données en cause sont localisés et de prendre des garanties pour que les droits et obligations prévus par la présente directive soient effectivement respectés ».

données personnelles. Les sociétés traitant des données personnelles ayant les capacités techniques de le faire en tout point du globe, il a fallu préciser le champ d'application territorial des mesures en question. Les jurisprudences nationales et européennes se sont donc prononcées sur l'appréciation concrètes des critères relatifs à l'établissement du responsable de traitement ou aux moyens de traitement mis en œuvre **(1)**, à l'heure ou de nouveaux critères de rattachement ont également été précisés par le RGPD **(2)**.

1. L'influence de la jurisprudence

499. Comme le révèle la doctrine, « avant l'arrêt *Google Spain*, la question de l'application du droit de l'Union aux sociétés collectant massivement des données sur les citoyens mais ayant leur siège en Californie se posait » et ce d'autant plus que « les internautes du monde entier, qui utilisent tous les jours les services proposés par Google ou Facebook, valident des conditions générales qui font référence à la loi californienne beaucoup moins protectrice que le droit français »[961]. La jurisprudence, notamment française, a eu vocation à se prononcer sur l'appréciation des critères relatifs au champ d'application territorial des règles contenues au sein de la règlementation protectrice des données personnelles. De façon relativement surprenante, celle-ci a d'abord retenu une conception restrictive de la notion d'établissement, telle qu'elle était entendue par la directive et par la loi de 1978 modifiée. Le tribunal de grande instance de Paris avait en effet arrêté cette position par une ordonnance de référé en date du 14 avril 2008[962].

En l'espèce, une personne française demandait la suppression de messages la concernant et publiés par elle sur un forum de discussion proposé et hébergé par le moteur de recherche *Google*. La demanderesse soutenait ainsi que les statuts de la société *Google France* confirmaient l'existence de moyens de traitement sur le territoire français. L'ordonnance de référé, fondée notamment sur l'article 4 de la directive et sur l'article 5 de la loi Informatique et Libertés, considérait pourtant que la société Google n'était pas établie en France et surtout, qu'elle n'utilisait pas de

[961] Anne Debet, Jean Massot, Nathalie Metallinos, *op. cit.*, p. 210.
[962] TGI Paris, référé, 14 avril 2008, *Madame X c/ Google.*

moyens de traitement sur le territoire français. Le tribunal a considéré que le site google.fr, à partir duquel les messages étaient envoyés et consultés, avait pour éditeur la société Google Inc. mais qu'il n'était pas démontré que la filiale française intervenait dans le processus de traitement des données. Cela empêchait dès lors de considérer que la société Google Inc. était établie en France ou utilisait des moyens matériels ou humains de la société Google France ou de toute autre entité située sur le territoire français.

La demanderesse faisait également valoir que la législation de l'Etat de Californie, en raison notamment du caractère sectoriel de celle-ci, ne lui permettait pas d'assurer ses droits et d'obtenir la suppression des messages litigieux. Pourtant, le TGI de Paris a considéré que la législation de cet Etat avait en réalité vocation à s'appliquer, « en raison de la production sur le territoire de l'Etat de Californie du fait générateur du dommage allégué, soit l'archivage de messages » diffusés sur des forums de discussion. Cette solution a pu sembler surprenante en raison du refus par le juge d'adopter une interprétation extensive de la notion d'établissement.

500. Les juridictions ont cependant dû adopter une solution différente pour se conformer à l'arrêt *Google Spain* de la CJUE[963]. Celui-ci, rendu en 2014, est révélateur de la volonté de la Cour de justice de garantir aux citoyens européens des moyens de recours effectifs lorsqu'ils sont concernés par des traitements de données trouvant leur source aux Etats-Unis. Dans cet arrêt, la CJUE était saisie d'une demande de décision préjudicielle faisant suite à un litige dans lequel un citoyen espagnol avait introduit une réclamation visant à faire disparaître des pages du moteur de recherche, des résultats relatifs à une saisie pratiquée en recouvrement de dette de sécurité sociale le concernant[964]. La question posée à la Cour de justice portait notamment sur le fait de savoir si la directive 95/46/CE était applicable à un exploitant de moteur de recherche ne se situant pas sur le territoire d'un Etat membre de l'Union. Pour y répondre, la Cour a d'abord considéré que *Google Spain* était une

[963] Anne Debet, Jean Massot, Nathalie Metallinos, *op. cit.*, p. 204.
[964] CJUE, gr. ch., 13 mai 2014, *Google Spain SL, Google Inc. c. Agencia Espanola de la Proteccion de Datos et Mario Costeja Gonzalez*, aff. C-131/12 ; AJDA 2014. 1147, chron. M. Aubert, E. Broussy et H. Cassagnabère ; D. 2014. 1476, note V.-L. Benabou et J. Rochfeld ; *ibid.* 1481, note N. Martial-Braz et J. Rochfeld ; *ibid.* 2317, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; *AJCT* 2014. 502, obs. O. Tambou ; *Constitutions* 2014. 218, chron. D. de Bellescize ; *RTD eur.* 2014. 283, édito. J.-P. Jacqué ; *ibid.* 879, étude B. Hardy ; *ibid.* 2016. 249, étude O. Tambou ; *Rev. UE* 2016. 597, étude R. Perray.

filiale de *Google Inc.* Elle a ensuite considéré « que le traitement de données à caractère personnel par le responsable de celui-ci est bien effectué dans le cadre des activités d'un établissement appartenant à ce même responsable et situé dans un Etat membre »[965]. La directive a donc été appliquée, étant donné que les activités de *Google Inc*. et de *Google Spain* étaient « indissolublement liées », la filiale espagnole gérant des activités publicitaires indispensables pour garantir la rentabilité économique du moteur de recherche. Cette solution, visant à adopter une interprétation large du critère d'établissement permettant d'y rattacher l'application de la directive de 1995, a été confirmée par la suite[966]. Ainsi, la Cour a pu considérer que la notion d'établissement au sens de la directive s'étendait à « toute activité réelle et effective même minime, exercée au moyen d'une installation stable »[967], jugeant ainsi que la présence d'un seul agent pouvait constituer une installation[968].

501. La jurisprudence nationale a également eu vocation à se prononcer sur l'appréciation du critère alternatif relatif aux moyens du traitement. Une décision du tribunal de commerce de Paris a permis d'apporter certains éclairages quant à l'interprétation, par les juridictions internes, des conditions relatives à la mise en œuvre d'un tel critère[969]. En l'espèce, la solution retenue concernait l'appréciation du statut des cookies laissés par le moteur de recherche sur les ordinateurs des individus. Le tribunal a retenu la qualification de « moyens » pour désigner les cookies employés par le moteur de recherche, la notion de « moyens » devant être interprétée dans un sens large. La particularité de cette décision a notamment été de faire directement référence à l'avis 1/2008 du G29 qui a considéré que la notion de moyens recouvrait l'ensemble des moyens, automatisés ou non, utilisés sur le territoire d'un Etat membre, à des fins de traitement de données à caractère personnel. La position retenue par le tribunal s'est dès lors inscrite dans la lignée de celle, extensive, adoptée par la CNIL. Ces solutions, assurant une application large des règles issues

[965] Marion Polidori, « L'arrêt Google Spain de la CJUE du 13 mai 2014 et le droit à l'oubli », *Civitas Europa*, vol. 34, no. 1, 2015, pp. 243-266.
[966] CJUE, 1er octobre 2015, aff. C-230/14, *Weltimmo s.r.o. c/ Nemzeti Adatvédelmi és Információszabadság Hatóság*, *AJDA* 2015. 2257, chron. E. Broussy, H. Cassagnabère et C. Gänser *; D.* 2015. 2011 *; ibid.* 2016. 1045, obs. H. Gaudemet-Tallon et F. Jault-Seseke *; Dalloz IP/IT* 2016. 47, obs. N. Metallinos *; JCP E* 2015. Actu. 767 ; *RLDI* nov. 2015, n° 3861, obs. L. Costes ; *CCE* 2015. Comm. 101, note A. Debet *; Europe* 2015. Comm. 470, obs. E. Daniel.
[967] Anne Debet, « Arrêt Weltimmo : un nouvel élargissement par la CJUE de la notion d'établissement », *Communication Commerce électronique*, décembre 2015, n°12.
[968] Nathalie Metallinos, « Données personnelles : la CJUE renforce les règles de protection », *Dalloz IP/IT*, 2016, p. 47.
[969] Tribunal de Commerce de Paris, 1ère chambre, 28 janvier 2014, *M. X c/ Google Inc., Google France.*

de la directive de 1995 et de la LIL, ont permis une appréhension des échanges réalisés dans le cadre de l'automesure et l'adoption du RGPD a permis d'établir un nouveau critère d'application territorial de la réglementation.

2. L'influence du Règlement européen

502. Le critère de l'activité dirigée ou ciblée. Le RGPD précise, dès son article 3, l'étendue de son champ d'application territorial. Celui-ci reprend les critères relatifs d'une part à l'établissement d'un responsable de traitement, auquel il ajoute également celui du sous-traitant, et d'autre part celle relative à l'application d'une règle de droit international public. Il vient également redéfinir le critère fondé sur l'identification géographique des moyens mis en œuvre. Celui-ci disparaît au profit d'un critère dit « d'activité dirigée » ou « activité ciblée » afin d'entraîner un élargissement exponentiel du champ d'application territorial[970]. Ainsi, l'article 3, 2° du Règlement dispose que celui-ci s'applique « au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union », lorsque les activités de traitement sont liées soit « à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes » ou « au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union ».

Ces nouveaux critères, larges dans leur principe en raison de l'ajout du sous-traitant aux différents critères d'application, sont précisés par les considérants 23 et 24 du texte. Dans un premier cas, pour déterminer si un responsable du traitement ou sous-traitant offre des biens ou des services à des personnes concernées qui se trouvent dans l'Union, « il y a lieu d'établir s'il est clair que le responsable du traitement ou le sous-traitant envisage l'offre des services à des personnes concernées dans un ou plusieurs Etats membres de l'Union ». Dans un second cas, il faudra déterminer si une activité de traitement est considérée comme un suivi du comportement et donc « établir si les personnes physiques sont suivies sur Internet »,

[970] Romain Perray, « La délimitation territoriale du RGDP : le champ d'application et les transferts de données hors de l'Union européenne », *Dalloz IP/IT*, 2016, p. 581.

ce qui comprend notamment, à l'image des dispositifs d'automesure, « l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit ».

503. Reprenant les règles européennes du droit de la consommation relatives à l'activité dirigée et au ciblage[971], ces critères permettent d'appliquer le RGPD dès lors que les données collectées sont relatives à une personne résidant dans l'Union européenne, ce qui démontre la volonté du législateur européen d'instaurer une application extraterritoriale des règles de protection. Ainsi, plutôt que de fonder la solution sur la localisation des moyens employés pour le traitement, la localisation des personnes concernées par de tels traitements permettra l'application du Règlement. Une telle solution manifeste dès lors clairement la « volonté de donner au règlement le champ d'application le plus large possible », en lui permettant de soumettre « les sociétés établies dans les Etats tiers mais actives sur le marché européen » aux mêmes règles que les sociétés européennes, correspondant à l'idée d'une protection des données personnelles « conçue comme un droit fondamental »[972]. Ces solutions, qui entraînent des capacités d'applications exponentielles des règles européennes relatives à la protection des données et qui s'inscrivent dans la lignée des solutions jurisprudentielles précédemment dégagées – par les arrêts *Google Spain* et *Weltimmo* notamment[973] – s'accompagnent également de moyens d'actions renouvelés, qu'il s'agisse de ceux des autorités nationales de contrôle ou des juridictions.

§2. Un décloisonnement des moyens de contrôle

504. Le champ d'application territorial de la règlementation est l'élément déterminant pour établir la loi applicable à un traitement de données. Mais la question

[971] V. art. 15 du Règlement 44/2001, 22 déc. 2000, Bruxelles I (art. 17 Règlement. 1215/2012, 12 déc. 2012, Bruxelles I bis) et 6 Règlement Rome I.
[972] Fabienne Jault-Seseke, Célia Zolynski, « Le règlement 2016/679/UE relatif aux données personnelles », *Recueil Dalloz*, 2016, p. 1874
[973] Romain Perray, « De la (bonne ?) application de la jurisprudence Weltimmo au bénéfice... d'Amazon et de Facebook », *Revue de l'Union européenne*, 2016, p.597.

de la compétence territoriale des autorités de protection et des juridictions en charge de faire appliquer la réglementation doit également être soulevée. En effet, des règles d'attribution de compétence différentes sont susceptibles de se présenter, notamment pour les cas ou des traitements de données ont un caractère transfrontalier, interne ou externe à l'Union européenne. Dès lors, d'éventuels divergences de solutions en cette matière risquent de compliquer les voies de recours offertes à des individus concernés par des traitements de données à caractère personnel. Les différents textes en vigueur ont progressivement procédé à une redéfinition de la compétence des autorités de contrôle **(A)**, mais également à une précision de la compétence des juridictions **(B)**.

A. La redéfinition de la compétence des autorités de contrôle

505. Les textes internes puis communautaires ont institué des autorités de contrôles indépendantes visant à contrôler la mise en œuvre des traitements. Pour exercer leurs attributions, elles ont bénéficié d'une compétence territoriale s'exerçant en théorie sur le territoire de l'Etat membre dont elles relevaient. Pourtant, ces autorités de contrôle ont été confrontées au caractère transfrontalier des échanges mis en œuvre. L'enjeu, dans le cadre du *quantified-self,* est de pouvoir déterminer avec précision quelle autorité de contrôle sera compétente. En effet, l'hypothèse de conflits entre différentes autorités, susceptible d'amoindrir la portée des droits des individus, est apparue. La compétence précisément encadrée des autorités nationales de contrôle a permis d'éviter de tels conflits **(1)** et certaines évolutions, liées aux notions d'autorité chef de file et de guichet unique, ont été introduites **(2)**.

1. Une compétence encadrée

506. L'article 28 de la directive de 1995 relatif aux autorités de contrôle ne donnait *a priori* que peu d'indications sur la compétence territoriale attribuée à celles-ci. Tout au plus, celui-ci indiquait en son point 6° que chaque autorité de contrôle avait « compétence pour exercer sur le territoire de l'Etat membre dont elle relève, les pouvoirs dont elle est investie ». Une précision était apportée sur le fait que chaque autorité pouvait être appelée à exercer ses pouvoirs sur demande d'une autorité d'un autre Etat membre, celles-ci coopérant entre elles dans la mesure

nécessaire à l'accomplissement de leurs missions, notamment par l'échange d'informations utiles. Dès lors, une autorité nationale de contrôle telle que la CNIL devait pouvoir exercer ses pouvoirs sur le territoire national, précision faite que ces autorités pouvaient être amenées à collaborer.

507. Les précisions. La loi Informatique et Libertés est venue apporter un certain nombre de précisions quant à la compétence territoriale dont était investie la CNIL. Ainsi, l'article 48 de la loi de 1978 modifiée en 2004 indiquait que celle-ci pouvait exercer ses pouvoirs à l'égard des traitements dont les opérations étaient « mises en œuvre, en tout ou partie, sur le territoire national, y compris lorsque le responsable du traitement était établi sur le territoire d'un autre Etat membre de la Communauté européenne ». Dès lors, l'autorité administrative indépendante était susceptible d'exercer ses pouvoirs (vérifications, contrôles sur pièce et sur place, prononcé de sanctions administratives ou pécuniaires ou encore injonctions de cesser le traitement) non seulement lorsqu'une partie au moins du traitement avait lieu sur le territoire national mais également lorsque le responsable de traitement était établi à l'étranger, à condition qu'il soit situé sur le territoire d'un Etat membre. Cet article soulevait cependant une question relative à l'appréciation de la notion « d'opération » utilisée par le texte. En l'absence de précisions de la loi et sans indications de la part de la CNIL, il semblait en effet difficile de savoir à quoi le texte faisait exactement référence et s'il fallait recourir à la notion de « moyens de traitement » pour définir le champ d'application territoriale de la loi.

508. Le mécanisme de coopération. Cette disposition, qui permettait de faciliter l'effectivité des contrôles et sanctions de la CNIL et de prévenir des conflits de lois entre Etats membres[974], pouvait également s'expliquer par les différentes marges de manœuvre laissées aux Etats dans la transposition de la directive de 1995. Cet instrument a en effet permis de procéder à une ébauche d'harmonisation des législations mais il a également pu créer des dissensions entre les différentes réglementations nationales en raison du mécanisme même de la transposition. Dès lors, précisément pour éviter que de telles différences empêchent de procéder à une application cohérente de la législation, l'ancien article 49 de la loi de 1978 a

formalisé le mécanisme de coopération préconisé par la directive en indiquant notamment qu'une autorité de protection d'un autre Etat membre pouvait demander à la CNIL de « procéder à des vérifications », « prendre les décisions » relatives aux sanctions ou encore « communiquer les informations qu'elle recueille ou qu'elle détient […] aux autorités exerçant des compétences analogues aux siennes dans d'autres Etats membres de la Communauté européenne ».

Cette hypothèse concernait la collaboration entre autorités de protection de différents Etats membres et la loi du 7 octobre 2016 a prévu l'hypothèse d'une collaboration entre la CNIL et une autorité équivalente dans un Etat non-membre de l'Union européenne mais présentant un niveau de protection adéquat. Ce procédé, soumis à la condition relative à la constatation du niveau de protection adéquat, a permis de renforcer les modalités de coopération et d'intervention au niveau international, tel que le souhaitait la Commission européenne. Cette dernière, dans une décision de 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers, indiquait que « les parties conviennent que l'autorité de contrôle a le droit d'effectuer des vérifications chez l'importateur de données et chez tout sous-traitant ultérieur dans la même mesure et dans les mêmes conditions qu'en cas de vérifications opérées chez l'exportateur de données conformément au droit applicable à la protection des données »[975]. Ces modalités n'ont pas eu pour effet de doter la CNIL d'une compétence internationale, mais celle-ci a pu, avant la redéfinition de ses attributions par le RGPD, bénéficier d'un domaine d'intervention important.

2. Une compétence renouvelée

509. Le recours à la notion d'établissement principal. Le Règlement général européen reprend à son compte l'institution d'une autorité de contrôle chargée de « contribuer à l'application cohérente du présent règlement dans l'ensemble de

[974] Anne Debet, Jean Massot, Nathalie Metallinos, *op. cit.* p. 209.
[975] Décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil, C (2010) 593, 2010/87/UE, clause n°8, 12 février 2010, JOUE.

l'Union » selon son article 51. Il introduit également deux nouveautés relatives au mécanisme de l'autorité chef de file et à la mise en œuvre d'un guichet unique. Ces hypothèses ont vocation à s'appliquer notamment pour les cas ou des traitements transfrontaliers de données sont mis en œuvre et impliquent que seule l'autorité de contrôle nationale de l'Etat dans lequel le responsable de traitement a son établissement principal soit compétente pour l'ensemble des litiges relatifs à ces traitements illicites[976]. Ainsi, comme le mentionne l'article 56 du Règlement, « l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable de traitement ou ce sous-traitant ». L'objectif est de pouvoir, à travers ce recours à la notion d'établissement principal en cas de transferts transfrontaliers, remédier à un éventuel manque de collaboration entre les différentes autorités de protection des données.

510. Les précisions. Le processus de nomination d'une autorité chef de file n'ayant de raison d'être que pour les cas de transferts transfrontaliers de données personnelles, il est nécessaire de préciser cette notion, au regard de l'article 4, point 23) du Règlement général. Celui-ci donne ainsi deux définitions du traitement transfrontalier. Il peut s'agir d'une part d'un « traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs Etats membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs Etats membres ». D'autre part, il peut s'agir d'un « traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs Etats membres ». La question du cadre des activités d'établissements ne pose en théorie pas de problèmes d'interprétation mais la référence au traitement

[976] Nathalie Martial-Braz, « L'extraterritorialité des décisions des autorités de régulation nationales : gage d'efficacité de la protection des données personnelles en Europe », *Revue de l'Union européenne*, 2016, p. 288.

qui « affecte sensiblement » a cependant nécessité des précisions, notamment de la part du groupe de l'article 29.

Celui-ci fait référence à cette notion dans ses lignes directrices sur l'autorité de contrôle chef de file en se référant à la version anglaise du texte et à l'appréciation des termes « *substantial* » et « *affect* ». Ceux-ci impliquent pour lui que « pour qu'un traitement de données affecte une personne, il faut qu'il ait une quelconque incidence sur cette dernière », et notamment une incidence significative[977]. Surtout, ce traitement peut également être simplement susceptible d'avoir une telle incidence. Le G29 liste un certain nombre de facteurs en fonction desquels les autorités de contrôle pourront retenir qu'un traitement « affecte sensiblement » un individu. Relatifs au dommage, à la perte, à des difficultés pour l'individu ou encore à une limitation éventuelle de ses droits, ces facteurs sont sujet à une appréciation *in concreto* de la part des autorités de contrôle. Le groupe de l'article 29 indique également que l'autorité de contrôle chef de file est « l'autorité qui assume la responsabilité principale de la gestion d'une activité de traitement transfrontalier », notamment « lorsqu'une personne concernée introduit une réclamation concernant le traitement de ses données à caractère personnel ».

511. Les limites. Le mécanisme du guichet unique, s'il a pour objectif de simplifier le mécanisme de contrôle, présente cependant certains inconvénients. En effet, bien qu'il vise au renforcement de la coopération entre les différentes autorités de protection, telle qu'elle était déjà imaginée par la directive de 1995, celui-ci est susceptible de favoriser la pratique du *forum shopping*, « à l'initiative des responsables de traitement ou de sous-traitants, et ce en faveur d'Etats membres dans lesquels les autorités de régulation seraient jugées, à tort ou à raison, plus clémentes »[978]. Cette solution du recours à l'établissement principal du responsable du traitement ou du sous-traitant « pourrait aboutir à terme à une concentration de la régulation entre les mains de quelques autorités de contrôle »[979]. Les responsables de traitement opérant dans le domaine du *quantified-self*, conscients que l'autorité

[977] G29, Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant, Adoptées le 13 décembre 2016, Version révisée et adoptée le 5 avril 2017, 16/FR, WP 244 rev.01, p. 3.
[978] Nathalie Martial-Braz, *art. précité*., p. 289.

administrative d'un Etat adopte des solutions clémentes, pourraient ainsi décider de fixer leur établissement dans cet Etat. Cette solution semble cependant devoir être tempérée par la nature même de l'instrument utilisé pour fixer les règles relatives à la protection des données personnelles. En effet, le règlement étant d'application directe et ne nécessitant pas de transposition, contrairement à une directive, les divergences entre les différentes législations nationales devraient être moindres même si les législateurs nationaux restent compétents pour fixer les règles relatives à leurs autorités de contrôle nationales. La compétence des autorités contrôle a eu vocation à évoluer progressivement et il en va de même pour celles des tribunaux, en dehors cette fois de tout cadre législatif ou réglementaire.

B. Une redéfinition de la compétence des tribunaux

512. Les juges nationaux et européens, prenant conscience des enjeux relatifs au numérique, notamment en matière de protection des droits fondamentaux, se sont emparés du sujet de la protection des données dans l'optique d'accroître le spectre d'application des règles protectrices des individus. Le décloisonnement des droits nationaux a ainsi eu pour objet de faire en sorte que l'application des règles relatives au numérique ne soit pas freinée par le caractère mondialisé des échanges. Le cyberespace a en effet procédé à une modification du rapport aux frontières terrestres et les juridictions ont dès lors tenté de maîtriser les potentiels effets néfastes résultant de ce phénomène. Cette influence juridictionnelle grandissante a d'abord eu lieu sous l'impulsion du juge national **(A)** pour ensuite être réaffirmée au niveau européen **(B)**.

1. La solution du juge national

513. La question de la compétence juridictionnelle. La compétence juridictionnelle vise à déterminer quelle sera la juridiction compétente pour statuer sur un éventuel litige. Cette compétence, en matière de protection des données personnelles, est théoriquement liée au régime juridique déterminé. Mais il peut

[979] Mihaela Ailincai, « Espoirs et inquiétudes autour de la révision du cadre juridique général de l'Union européenne sur la protection des données à caractère personnel », *Revue de l'Union Européenne*, 2014, p. 170.

arriver dans certains cas que « le droit applicable et la compétence judiciaire ne soient pas les mêmes pour un traitement donné »[980]. Une des difficultés majeures à laquelle peuvent se heurter les internautes, utilisateurs potentiels de dispositifs d'automesure connectés, pour que soient respectés leurs droits, est d'attraire un éventuel défendeur devant un tribunal français qui se déclare compétent pour appliquer la réglementation française protectrice des données personnelles. Les critères classiques de rattachement relatifs à l'établissement et aux moyens semblent en principe larges mais ceux-ci sont susceptibles de faire l'objets de certaines restrictions venant des entreprises elles-mêmes.

514. Le contournement des règles de compétence. Nonobstant les règles visant à déterminer la loi applicable, la majorité des entreprises du numérique installées outre-Atlantique insèrent dans leurs conditions générales d'utilisation des clauses relatives à la compétence territoriale des tribunaux en cas de litige. Dès lors, il est possible de constater que, pour une majorité d'entre elles, « aucune de ces sociétés ne propose d'emblée, de manière claire et explicite, à l'utilisateur résidant en France un contrat soumis au droit français »[981]. Surtout, celles-ci font généralement référence à la compétence des juridictions du comté de Santa-Clara en Californie, qualifié à cette occasion de « Santa-Clara sur Seine » par certains auteurs, pour rappeler qu'en cas de litiges, notamment sur le territoire français, ceux-ci devraient être portés à la connaissance des juridictions du comté californien[982]. Le réseau social Facebook avait, avant l'adoption du RGPD, recours à ce type de procédé dans ses conditions générales d'utilisation :

> *« Vous porterez toute plainte afférente à cette Déclaration ou à Facebook exclusivement devant les tribunaux d'État et fédéraux sis dans le comté de Santa Clara, en Californie. Le droit de l'État de Californie est le droit appliqué à cette Déclaration, de même que toute action entre vous et nous, sans égard aux principes de conflit de lois. Vous acceptez de respecter la juridiction des*

[980] G29, avis n°8/2010, *op. cit.*, p. 11.
[981] Olivier Iteanu, *Quand le digital défie l'Etat de droit*, Editions Eyrolles, septembre 2016, p. 15.
[982] Alex Türk, *La vie privée en péril. Des citoyens sous contrôle*, Odile Jacob, Avril 2011, 272 p.

tribunaux du comté de Santa Clara, en Californie, dans le cadre de telles actions »[983].

Ces clauses attributives de compétence ont été, avec l'avènement des réseaux sociaux et du web relationnel, rapidement portées à la connaissance des juridictions françaises. Certaines clauses n'ont pas été écartées en raison de l'absence de traitement directement réalisé sur le territoire français[984] mais la jurisprudence a progressivement eu tendance à les censurer de manière automatique, en raison de leur caractère abusif. Ainsi, la Cour d'appel de Pau a jugé en 2012 que la clause d'attribution de compétence des juridictions californiennes intégrées aux conditions générales d'utilisation de *Facebook* était abusive et donc non-opposable aux consommateurs[985]. Un nouveau litige concernant le réseau social a permis à la Cour d'appel de Paris d'adopter en 2016 une position similaire et de confirmer le caractère abusif et réputé non-écrit de la clause en question[986]. Cette solution, fondée sur le droit de la consommation[987], implique dès lors que les litiges susceptibles de survenir soient traités par le tribunal du lieu où le consommateur est domicilié. Le réseau social a cherché à contester son activité commerciale mais la Cour a retenu que « la société Facebook Inc. retire des bénéfices importants de l'exploitation de son activité », fondée sur l'utilisation de données à caractère personnel transmises par la personne concernée. Il est possible de constater, dans le prolongement de ces différentes décisions, que les clauses litigieuses mises en œuvre ont eu tendance, non pas à disparaître, mais à recourir de manière subsidiaire à la compétence des tribunaux californiens, pour les cas où la loi du pays de résidence de la personne concernée ne l'exclurait pas.

515. L'application au *quantified-self*. Par ailleurs, alors que cette problématique ne semble concerner au premier abord que les réseaux sociaux ou les

[983] Paragraphe 16 alinéa 1 des Conditions générales d'utilisation, version abrogée.
[984] TGI Paris, référé, 14 avril 2008, *Madame X c/ Google* ; En l'espèce, le Tribunal de Grande Instance de Paris a considéré que la législation de l'Etat de Californie avait en réalité vocation à s'appliquer, « en raison de la production sur le territoire de l'Etat de Californie du fait générateur du dommage allégué, soit l'archivage de messages » diffusés sur des forums de discussion.
[985] Cour d'appel de Pau, 23 mars 2012, *Sébastien R./Facebook*, n° 11/03921, *Dalloz actualité*, 16 avr. 2012, obs. C. Manara ; *RDC* 2012. 1340, obs. E. Treppoz ; *Gaz. Pal.* 17 mai 2012, n° 138, p. 11, obs. F. de Bérard.
[986] Cour d'appel de Paris, 12 février 2016, *Facebook Inc./Monsieur X*, n° 15/08624.
[987] Notamment sur les articles 15 et 16 du Règlement (CE) n° 44/2001 du conseil du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale.

moteurs de recherche, la question de l'utilisation de telles clauses par des entreprises opérant dans le domaine du *quantified-self* est susceptible de se poser. Ainsi, le constructeur d'objets connectés et développeur d'applications *FitBit* indique au sein de ses conditions générales d'utilisation que les litiges devront, sauf exceptions requises par les lois applicables, les litiges portant sur l'utilisation des services proposés par cette société devront être portés devant les tribunaux californiens[988]. Il ne fait pourtant pas de doute qu'au regard des solutions précédemment dégagées, les tribunaux français se reconnaîtront compétents pour connaître d'éventuels litiges relatifs à un tel service. Surtout, en dehors de l'influence du juge français, le juge européen s'est aussi engagé dans la voie d'une protection uniformisée des personnes concernées par un traitement de données personnelles.

2. La solution du juge européen

516. La Cour de justice de l'Union européenne s'est également prononcée quant à la détermination de la juridiction compétente. La question posée ne concernait pas directement le caractère abusif d'une éventuelle clause attributive de juridiction mais nécessitait en revanche de savoir si un individu souhaitant agir contre une entreprise du numérique située sur le territoire de l'Union devait le faire auprès de la juridiction de l'entreprise, ou s'il pouvait exercer cette action auprès du tribunal de son lieu de résidence. La solution retenue s'est à nouveau fondée sur l'application des règles du droit de la consommation, telles qu'elles sont issues du droit européen et du Règlement Bruxelles I aux termes duquel un défendeur doit en principe être attrait devant les juridictions de l'Etat membre dans lequel il habite ou a son siège[989].

517. Le « for du consommateur » écarté. La question posée à la Cour portait ainsi sur le fait de savoir si une juridiction (autrichienne en l'espèce) était compétente pour connaître d'un litige relatif à une société dont le siège était basé en Irlande[990]. Pour y répondre, la Cour de justice a d'abord dû déterminer si le requérant était bien

[988] « Except as otherwise required by applicable law, the Terms of Service and the resolution of any Disputes shall be governed by and construed in accordance with the laws of the State of California without regard to its conflict of laws principles ».
[989] Règlement (CE) n° 44/2001 du Conseil, du 22 décembre 2000, concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale.
[990] CJUE, 25 janvier 2018, aff. C-498/16, *Maximilian Schrems c/ Facebook Ireland Limited.*

un consommateur au sens de la directive, qualification qu'elle a effectivement retenue. Pourtant, elle a écarté l'application du Règlement au motif que le « for du consommateur », règle permettant à celui-ci d'attraire un partenaire contractuel étranger devant les tribunaux de son domicile, ne pouvait être invoquée en raison de la nature de l'action intentée. Le consommateur, en l'espèce, faisait valoir ses propres droits mais également ceux d'autres personnes lui ayant cédé le droit de faire valoir leurs prétentions dans le cadre d'une action de groupe. La Cour a dès lors indiqué que la notion de « for du consommateur » avait été créée dans le but de protéger la partie au contrat en cause et que sa protection n'était assurée que dans le cas où il était « personnellement demandeur ou défendeur dans une procédure »[991]. Dès lors et *a contrario*, si celui-ci ne pouvait engager une action en tant que « cessionnaire de droits d'autres consommateurs », celui-ci aurait pu engager une action individuelle et obtenir gain de cause.

518. L'application au *quantified-self*. Une telle solution, fondée sur le droit de la consommation et relative à la compétence des juridictions d'Etats-membres, trouve un certain écho en matière de *quantified-self*. Elle permet en effet de clarifier les rapports entre la personne concernée par un traitement de données, utilisatrice d'un dispositif connecté et son contractant. Il est ainsi possible de mentionner l'exemple de la société *Withings*, société française proposant à la vente des objets connectés dédiés au *quantified-self* (montres, bracelets ou balances connectés reliés à des applications de suivi). Celle-ci, avant d'être à nouveau racheté par son fondateur en 2018, a fait l'objet d'un rachat par la firme finlandaise *Nokia* en 2016. Les conditions générales d'utilisations relatives à ces services connectés mentionnaient alors que « sauf disposition légale contraire et impérative, tout litige relatif aux présentes Conditions Générales d'Utilisation des Services Nokia ainsi que tout litige s'y rapportant est soumis au tribunal compétent du ressort d'Helsinki (Finlande) et soumis à la loi applicable en Finlande »[992]. L'application de la solution retenue par la CJUE en 2018 permettait cependant de passer outre cette clause pour offrir la possibilité à l'utilisateur d'attraire la firme devant les juridictions de son lieu de

[991] CJUE, Communiqué de presse n° 7/18, Arrêt dans l'affaire C-498/16, *Maximilian Schrems/Facebook Ireland Limited*, Luxembourg, 25 janvier 2018.
[992] https://health.nokia.com/fr/fr/legal/services-terms-and-conditions.

résidence. La société Withings, à nouveau établie en France, indique désormais que seules juridictions françaises sont compétentes en cas de litiges. La solution retenue par la CJUE en 2018 permettrait pourtant à un utilisateur résidant à étranger, en Belgique par exemple, d'attraire la firme devant les juridictions de son lieu de résidence.

519. Le rôle de la Commission. La commission est également intervenue dans le même sens : dans une communication en date de mars 2017, la Commission européenne a demandé aux entreprises de médias sociaux de se conformer au droit des consommateurs de l'Union, en demandant une clarification ou une suppression des conditions illégales, telles que celles permettant aux réseaux sociaux de « priver les consommateurs de leur droit de saisir la justice dans leur Etat membre de résidence »[993]. Cette requête, qui fait suite au constat similaire réalisé par la Direction générale française de la concurrence, de la consommation et de la répression des fraudes et par la Commission en novembre 2016[994], permet d'expliquer le recours désormais simplement subsidiaire à la loi californienne par les réseaux sociaux. Ces solutions, explicitées par le recours au droit de la consommation, permettent ainsi de compléter le dispositif mis en œuvre par la réglementation relative à la protection des données personnelles, celle-ci ayant eu vocation à être renouvelée par le RGPD. Ce dernier permet d'instaurer sur ce point, une réelle position européenne commune et procède surtout à l'établissement d'une nouvelle forme de régulation permettant un renforcement de la protection et une meilleure prise en compte des risques liés à la pratique de l'automesure.

520. Conclusion du chapitre. La pratique du *quantified-self* implique, pour être efficace, qu'un nombre important d'opérations soient réalisées. Différents acteurs, généralement situés en des lieux géographiques différents, sont ainsi appelés à collaborer et à s'échanger des données à caractère personnel. Cette situation est porteuse d'insécurité juridique pour les individus : des conflits de lois sont susceptibles d'apparaître, favorisés par les clauses attributives de compétence

[993] Commission européenne, *La Commission européenne et les autorités de protection des consommateurs des États membres demandent aux entreprises de médias sociaux de se conformer au droit des consommateurs de l'UE*, Communiqué de Presse, Bruxelles, 17 mars 2017.

auxquelles les différents responsables de traitement ont recours. Largement utilisées, ces clauses auraient pu, en raison de la nationalité des responsables de traitements opérant dans le domaine du *quantified-self,* permettre une concentration des litiges entre les mains des juges californiens. Les règles applicables à la détermination de la loi applicable et à la compétence territoriale des juridictions et autorités administratives ont cependant fait l'objet d'évolutions permettant d'éviter cette concentration. Désormais élargies, les critères de rattachement au droit européen garantissent aux personnes concernées la faculté de pouvoir exercer leurs droits, en dépit du caractère transfrontalier des échanges de données réalisés dans le cadre de l'automesure.

521. Conclusion du titre. L'automesure connectée, grâce aux dispositifs utilisés pour sa mise en œuvre, concentre un certain nombre d'innovations technologiques. Ces innovations, qui convergent toutes dans le sens d'un meilleur retour d'informations proposé à l'utilisateur, contribuent à la mise en œuvre de chaînes de traitements. Celles-ci reposent sur une double externalisation : structurelle (les individus transmettent leurs données à plusieurs prestataires) et géographique (les différents prestataires sont situés en des zones territoriales différentes). Le droit a donc dû évoluer pour garantir aux individus une protection cohérente sur l'ensemble de ces chaînes de traitement. Deux mouvements complémentaires ont progressivement permis d'assurer cette cohérence. D'abord, les différentes personnes appelées à traiter des données ont fait l'objet d'une identification plus précise. La clarification du rôle attribué aux sous-traitants par le RGPD a entrainé une meilleure maîtrise du risque informationnel en conférant des obligations à l'ensemble des personnes intervenant dans la chaîne de traitement. Procéder ainsi a permis d'éviter un éventuel délitement des droits des individus, à force de transferts successifs. Ensuite, le droit a dû prendre en compte le caractère transfrontalier des échanges. Procédant parfois de manière extensive, comme en témoigne l'arrêt *Google Spain* rendu par la CJUE en 2014, la jurisprudence a d'abord veillé à ce que les textes

[994] DGCCRF, European Commission, *Common position of national authorities within the CPC Network concerning the protection of consumers on social networks*, novembre 2016.

européens soient largement appliqués[995]. Le RGPD, par son champ d'application territorial étendu, a confirmé cette interprétation[996] en permettant une meilleure protection des données d'automesure lorsque celles-ci font l'objet de transferts. Cette application territoriale élargie du droit européen n'est cependant pas illimitée, comme en témoigne l'arrêt du la CJUE en date du 24 septembre 2019 qui a limité la portée du droit au déréférencement aux extensions européennes du moteur de recherche Google[997].

[995] Bruno Hardy, « Application dans l'espace de la directive 95/46/CE : la géographie du droit à l'oubli », *RTD eur*. 2014, p. 879.
[996] Alexis Deroudille, Farid Fatah, « L'extraterritorialité du RGPD dans le contexte du « *Cloud Act* » », *Rev. UE*, 2019, p. 442.
[997] CJUE, 24 septembre 2019, aff. C-507/17, *Google LLC. c/ Commission nationale de l'informatique et des libertés (Cnil).*

TITRE II – UNE NOUVELLE FORME DE RÉGULATION

522. Le transfert du rôle protecteur. Le nouveau Règlement européen entend mettre en place un cadre unique de protection. Sa particularité réside dans le « changement de paradigme »[998] mis en œuvre pour parvenir à protéger les données à caractère personnel. Le RGPD vise en effet à promouvoir une approche par les risques, censée permettre l'instauration d'un climat de confiance entre responsables de traitements, sous-traitants et personnes concernées par des traitements de données à caractère personnel. A ce titre, alors que la confiance devait auparavant émaner principalement de la réglementation et des normes législatives adoptées au niveau étatique, le texte européen fait des responsables de traitement des acteurs à part entière de cette régulation renouvelée. Un transfert du rôle protecteur peut en effet être constaté, de la législation et de l'Etat, vers les responsables de traitement. Cette délégation de la protection s'explique, dans le cas du *quantified-self*, par la technicité des moyens de collecte employés. Plutôt qu'un texte de portée générale aux dispositions abstraites, le nouveau cadre juridique, tout en étant neutre d'un point de vue technologique, confère aux responsables de traitement le soin d'assurer le respect des règles en vigueur, au regard notamment de l'évolution technique des traitements de données à caractère personnel.

Le flux d'informations collectées, favorisé par le recours à des objets connectés, impose de repenser le cadre protecteur apporté aux individus. L'impossibilité de maîtriser avec certitude l'ensemble des traitements réalisés a ainsi conduit la réglementation à favoriser, dans une logique de prévention des risques, le développement de mesures *ex ante* reposant largement sur les responsables de traitement. Cette responsabilisation des acteurs du numérique appelés à traiter des données à caractère personnel s'accompagne d'importants changement dans la mise en œuvre de la réglementation. Le RGPD entend ainsi favoriser le développement de

[998] CNIL, délibération n° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du janvier 1978.

la régulation, nécessaire au regard de la complexité des opérations réalisées et justifiée par la diversification des acteurs participant à l'élaboration et à l'application de normes. S'inscrivant dans un mouvement d'agencification[999], cette régulation nouvelle repose de plus en plus sur le recours à des instruments de droit souple qui permettent une meilleure prise en compte des spécificités propres au *quantified-self*.

523. Les problèmes posés par l'automesure connectée, qu'il s'agisse des difficultés liées à la qualification juridique des données collectées ou à la remise en cause des principes de protection, ont de plus en plus tendance à s'effacer. En effet, le RGPD, en favorisant le recours à des instruments de droit souple, entend mettre en œuvre une protection « à la carte » des données, en fonction des spécificités de chaque traitement. Le développement de ce droit souple doit également permettre aux responsables de traitement d'établir avec plus de certitude leur conformité à la réglementation. Les sanctions dissuasives qui sont instaurées doivent contribuer à assurer la protection des droits et libertés et ainsi favoriser le développement d'un environnement vertueux pour les individus concernés par des traitements de données à caractère personnel. Le développement de l'autorégulation, censé permettre une responsabilisation des responsables de traitement **(Chapitre I)**, s'inscrit de façon plus générale dans un mouvement de renouvellement de la régulation publique **(Chapitre II)**.

[999] Jacques Chevallier, *L'État post-moderne*, 4ème éd., LGDJ, 2017, p. 188.

CHAPITRE I – LE DÉVELOPPEMENT DE L'AUTORÉGULATION

524. Le système de protection des données à caractère personnel mis en œuvre depuis 1978 par la LIL, renouvelé en 2004 par la transposition de la directive de 1995, reposait sur une logique de déclaration administrative des traitements réalisés à la CNIL, chargée d'enregistrer la validité de telles opérations de collecte et de traitement. Cette logique déclarative, qui pouvait faire l'objet de nombreuses exceptions, permettait de juger de la légalité des opérations de traitement réalisées avant leur mise en œuvre. Elle ne permettait cependant pas d'assurer le suivi des traitements réalisés sur la durée. La CNIL était susceptible d'opérer un certain nombre de contrôles ou de prononcer des sanctions, mais ces mesures *ex post* étaient uniquement susceptibles de réparer ou d'arrêter un préjudice dont la réalisation n'avait pu être empêchée.

525. Les limites de la règlementation. La réglementation, ensemble de règles qui gouvernent une matière[1000], est en principe contraignante pour les personnes qui en sont destinataires[1001]. Fondée sur un ensemble de règles de droit figées et habituellement définies comme des règles de conduite générales, abstraites et obligatoires, dont la sanction est assurée par l'autorité publique[1002], la protection apportée aux données par cette réglementation a été remise en question par la pratique du *quantified-self*. La déclaration administrative préalable, associée à un régime juridique de protection *ex post*, n'a pas permis de limiter efficacement le risque informationnel pesant sur les individus ; les capacités exponentielles de collecte, la généralisation des transferts internationaux de données et les possibilités renouvelés d'interconnexion de fichiers, ont rendu nécessaire l'évolution du cadre juridique. La pratique de l'automesure participe ainsi de la reconstruction du droit à la protection des données, fondé aujourd'hui sur le recours à la régulation.

[1000] Gérard Cornu, *Vocabulaire juridique*, coll « Quadrige », 12ème éd., PUF, 2018, p. 605.
[1001] Franck Lagarde, « Réglementation, normalisation, certification, labellisation... : éléments de définition », *JS*, 2018, n°188, p.1.
[1002] Rémi Cabrillac, *Introduction générale au droit*, Dalloz, coll. « cours », 2007, p. 7.

526. Les différentes conceptions de la régulation. La notion de régulation ne fait pas l'objet d'une définition unifiée. Mais elle peut servir à qualifier le nouveau paradigme relatif aux évolutions du droit contemporain[1003]. Plusieurs théories doctrinales ont été fondées sur la notion de régulation. D'abord, la thèse du « droit-régulation » identifie des modes d'action souples et informels qui seraient dépourvus de caractère contraignant[1004]. Plusieurs instruments entrent dans cette catégorie, qu'il s'agisse des recommandations, des communications ou des circulaires. Ensuite, l'hypothèse d'un droit de la régulation a également été avancée, droit qui regrouperait « l'ensemble des règles affectées à la régulation de secteurs qui ne peuvent engendrer leurs équilibres par eux-mêmes »[1005]. Enfin, la thèse de l'Etat régulateur a été formulée, illustrant une vision de l'Etat qui se borne à imposer aux agents économiques « certaines règles du jeu et s'efforce d'harmoniser leur action »[1006]. Le mécanisme mis en œuvre par le RGPD ne semble coïncider directement avec aucune des thèses énoncées. Mais l'évolution progressive du droit de la protection des données semble emprunter des éléments à chacune de ces conceptions.

527. La minimisation des risques. De manière générale, l'objectif de la régulation, comparé à la réglementation, est de « minimiser les risques pour un niveau donné d'avantages »[1007]. En matière de protection des données personnelles, la régulation tend progressivement à la mise en œuvre de mesures de protection *ex ante* visant à prévenir en amont les risques pesant sur les individus quant à l'utilisation qui peut être faite de leurs données. Le développement de cette régulation, encouragé par le RGPD, doit permettre une maîtrise du risque réputationnel pesant sur les individus en garantissant la protection des données tout au long de la chaîne de traitement mise en œuvre. La régulation doit assurer à l'individu que ses données seront à tout moment traitées et utilisées conformément aux principes édictées par la réglementation, sous le contrôle direct des opérateurs du numérique qui vont jouer un rôle important en matière de prévention des risques relatifs à la vie privée.

[1003] Arnaud Séé, « Régulation (conceptions doctrinales) », *in* Michel Bazex, Gabriel Eckert, Régis Lanneau, Christophe Le Berre, Bertrand du Marais, Arnaud Sée (dir.), *Dictionnaire des Régulations*, Lexis Nexis, 2016, p. 515.
[1004] Gérard Timsit, « La régulation. La notion et le phénomène », *RFAP*, 2004, p. 5.
[1005] Marie-Anne Frison-Roche, « Le droit de la régulation », *Recueil Dalloz*, 2011, p. 611.
[1006] Jacques Chevallier, « L'Etat régulateur », *RFAP*, 2004, n° 111, p. 473.
[1007] Alain Rallet, Fabrice Rochelandet, « La régulation des données personnelles face au web relationnel : une voie sans issue ? », *Réseaux*, n°3, 2011.

528. Le changement de paradigme. Ce cadre juridique repensé repose sur un changement de paradigme quant aux règles protectrices mises en œuvre[1008]. Alors que le contrôle du respect de ces règles reposait auparavant exclusivement sur la CNIL, le nouveau cadre juridique entend responsabiliser les responsables de traitement, opérateurs de services numériques[1009]. Ces derniers ne sont plus seulement chargés d'appliquer un ensemble de règles sous le contrôle d'une autorité externe. Ils doivent désormais contribuer à l'élaboration des règles et vérifier eux-mêmes qu'ils respectent la réglementation applicable. Le contrôle opéré par la CNIL ne porte donc plus seulement sur la mise en œuvre des traitements mais il concerne également le respect, par les responsables de traitement, de leur conformité à la réglementation. Ces derniers sont donc chargés de prouver à tout moment que les traitements qu'ils réalisent sont conformes aux dispositions légales et que les mesures de protection des données à caractère personnel traitées sont respectées. Le développement de cette autorégulation s'inscrit dans un mouvement de responsabilisation des acteurs du numérique qui, s'ils demeurent en principe libres de traiter des données à caractère personnel pour la mise en œuvre des services qu'ils proposent, sont tenus de démontrer qu'ils y procèdent en toute légalité et dans le respect des mesures protectrices mises en œuvre.

La responsabilisation accrue des personnes chargées de réaliser des opérations sur des données à caractère personnel doit en théorie répondre à la problématique de la multiplication des traitements mis en œuvre. En effet, la diversité des opérations réalisées et le nombre croissant d'informations collectées rendent le contrôle de ces traitements difficile à mettre en œuvre en pratique. La mise en œuvre de procédés d'autorégulation doit permettre une meilleure appréhension des risques, qu'il s'agisse du défaut de loyauté du traitement réalisé, de la réutilisation excessive des données collectées, de la transmission non-autorisée de ces données à un tiers ou encore de la présence de failles de sécurité. Ces différents éléments sont difficilement décelables

[1008] Lucie Cluzel-Métayer, Emilie Debaets, « Le droit de la protection des données personnelles : la loi du 20 juin 2018 », *RFDA*, 2018, p. 1101.
[1009] Marie-France Mazars, Wafae El Boujemaoui, « Maîtriser le socle du droit de la protection des données pour aborder l'application du Règlement européen (RGPD) », *Rev. trav.*, 2018, p. 298 ; François Viney, « La loi relative à la protection des données personnelles », *AJ fam*, 2018, p. 366 ; Clémence Scottez, « Le RGPD, un nouveau paradigme de la protection des données personnelles pour les professionnels et le régulateur », *Dalloz IP/IT*, 2019, p. 229 ; Arnaud Lecourt, « RGPD : nouvelles contraintes, nouvelles stratégies pour les entreprises », *Dalloz IP/IT*, 2019, p. 205.

par une seule autorité de contrôle ou par les personnes concernées. Faire reposer la surveillance de ces paramètres sur les responsables de traitement permet de limiter la survenance de risques et d'éviter une application éparse des règles relatives à la protection des données. Les responsables de traitement, par le développement de l'autorégulation, deviennent acteurs de la protection des données qu'ils sont amenés à traiter et co-régulateurs du cadre juridique relatif à la protection des données.

529. La régulation favorisée par la technologie. Les objets employés pour la collecte et le traitement peuvent dans certains cas garantir que les données seront traitées en conformité avec la réglementation. Cette affirmation est susceptible de trouver un écho particulier en matière de *quantified-self*. Puisque celui-ci s'est automatisé et qu'il repose sur l'utilisation d'objets connectés à Internet généralement dotés de puces RFID, la configuration technique de ces objets contribue à la régulation en devenant un instrument de conformité. Représentant également une mesure de protection *ex ante*, cette adaptation au cadre juridique des outils techniques employés pour procéder au traitement de données à caractère personnel doit permettre une maîtrise plus efficace du risque informationnel pesant sur les individus.

Ainsi, cette redéfinition des modes de régulation qui pèse sur les acteurs privés **(Section 1)** s'accompagne d'une redéfinition des modes de régulation, opérée directement par la technologie utilisée **(Section 2)**.

SECTION I. LA CONTRIBUTION DES ACTEURS PRIVÉS A LA RÉGULATION

530. Le Règlement général européen entré en application le 25 mai 2018 opère un certain nombre de changements quant à la réglementation précédemment applicable. Les nouvelles mesures mises en œuvre visent ainsi à renouveler le rôle des responsables de traitement en matière de protection des données à caractère personnel. De nombreuses formalités préalables auprès de la CNIL ont eu vocation à disparaître et ce changement a pour contrepartie une nécessaire responsabilisation des acteurs du numérique. A ce titre, plusieurs grands principes protecteurs peuvent être dégagés du texte européen. Ceux-ci, novateurs, font du responsable de traitement un acteur à part entière de l'application du dispositif protecteur. Les acteurs privés, en charge notamment du déploiement de services de *quantified-self*, font donc l'objet d'obligations renouvelées, laissant de côté la logique déclarative qui prévalait jusqu'à maintenant. Une obligation de conformité à la réglementation pèse désormais sur les responsables de traitement **(Paragraphe 1)** et elle se double d'une obligation de transparence renforcée **(Paragraphe 2)**.

§1. La mise en œuvre d'une obligation de conformité

531. Le régime renouvelé mis en place par le RGPD repose majoritairement sur l'idée qu'un responsable de traitement doit être en mesure de prouver, à tout moment, qu'il agit en conformité avec la réglementation. Cette obligation, qui peut s'apparenter à une délégation du contrôle opéré aux entreprises elles-mêmes, permet notamment de saisir la problématique relative aux chaînes de traitement de données et aux risques de perte de maîtrise et de visibilité qui en découlent. Celle-ci doit également garantir aux individus que leurs données seront traitées conformément à la réglementation pendant toute la durée du traitement et non plus seulement lors de sa mise en œuvre. Plusieurs procédures nouvelles sont mises en œuvre par le RGPD, qui fait du responsable de traitement l'acteur principal de la protection des données à caractère personnel. Est ainsi favorisée, pour répondre au développement croissant

d'opérations de collecte et d'analyse, la mise en place de règles d'entreprise contraignantes **(A)**. Celles-ci sont complétées par un principe d'*accountability*, qui vise l'obligation pour les entreprises d'établir des procédures internes permettant de démontrer le respect des règles relatives à la protection des données à caractère personnel **(B)**.

A. Le développement de « binding corporate rules »

532. L'article 4, 20) du Règlement définit les règles d'entreprise contraignantes comme « les règles internes relatives à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire d'un Etat membre pour des transferts ou pour un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant établi dans un ou plusieurs pays tiers au sein d'un groupe d'entreprise, ou d'un groupe d'entreprises engagées dans une activité économique conjointe ». Ces règles d'entreprise contraignantes, illustrant le déplacement de la régulation opéré par le RGPD, sont directement instaurées par les responsables de traitement **(1)** afin de permettre une meilleure protection des données lorsque celles-ci font par exemple l'objet de transferts au sein de groupes d'entreprises **(2)**.

1. La création d'une réglementation interne

533. L'institutionnalisation des règles d'entreprise. La particularité du RGPD est de faire reposer une partie du dispositif protecteur directement sur les entreprises en charge de traiter des données à caractère personnel. Devenant acteurs majeurs de l'application effective de la réglementation et de la protection des données, ceux-ci sont appelés à suppléer, dans une certaine mesure, le rôle conféré à l'origine aux autorités administratives indépendantes en charge de la protection. A ce titre, les responsables de traitement sont appelés à devenir directement créateurs de règles internes protectrices des données des individus. Le cas des règles d'entreprise contraignantes représente en ce sens un apport significatif du Règlement européen puisqu'il permet à des entreprises d'adopter un ensemble de règles de nature obligatoire, un code de conduite venant définir les modalités de transferts de données

personnelles réalisés par une entreprise. Présentées comme une solution alternative aux clauses contractuelles types, le développement de ces règles internes était à l'origine fondé sur l'article 26, 2 de la directive de 1995, relatif aux dérogations permettant un transfert vers un pays tiers n'assurant pas un niveau de protection adéquat.

Les règles internes d'entreprises sont devenues, au fil du temps, un mécanisme juridique largement reconnu par les autorités de contrôle nationales et les entreprises multinationales. Outil efficace pour encadrer les transferts internationaux et pour faire face à la complexité et à la diversité des transferts de données au sein d'un groupe, celles-ci ont été perçues comme « une solution flexible – sur mesure – permettant de tenir compte des spécificités de chaque groupe d'entreprises et reposant sur des mécanismes déjà utilisés »[1010]. Ces règles d'entreprise ont notamment fait l'objet de certains développements de la part du groupe de l'article 29 ou encore de la CNIL au niveau national. Ce mécanisme faisait à l'origine l'objet d'une certaine méfiance, y compris de la part du G29, concernant la solidité des garanties apportées aux transferts internationaux de données[1011]. Mais l'institutionnalisation de ce mécanisme par les autorités protectrices a permis d'en pérenniser le recours et les effets, plusieurs documents présentant les exigences relatives à l'instauration de *binding corporate rules* ayant été adoptés[1012] et visant notamment à ce que celles-ci soient « respectées par toutes les entités du groupe, quel que soit leurs pays d'implantation, ainsi que par tous leurs salariés »[1013]. L'entreprise Philips, à l'origine en 2010 du service de *quantified-self* Direct Life permettant de mesurer son activité physique, a adopté des BCR dès 2012 afin d'encadrer les transferts entre les différentes entités du groupe[1014].

534. Des règles contraignantes. Les *binding corporate rules* permettent d'assurer la conformité des traitements aux éléments de la réglementation et d'uniformiser les pratiques relatives à la protection des données personnelles au sein

[1010] Anne Debet, Jean Massot, Nathalie Metallinos, *op. cit.*, p. 711.
[1011] G29, *Document de travail relatif aux transferts de données personnelles vers des pays tiers*, WP 74, 3 juin 2003, p. 5.
[1012] Voir par exemple G29, WP 133, WP153, WP 154 et WP 155.
[1013] CNIL, *Les règles internes d'entreprise ou BCR* (*binding corporate rules*), 2017, p. 2.
[1014] https://www.philips.com/c-dam/corporate/about-philips/investor-relations/General-Business-Philips PrivacyRulesCSBData.pdf

d'un groupe. Elles doivent ainsi revêtir, pour en garantir l'efficacité, un caractère contraignant permettant de définir un standard de protection des données, applicable non seulement au sein du groupe de sociétés (ce standard doit par exemple être applicable à tous les salariés du groupe) mais également à l'extérieur du groupe, à l'égard des personnes concernées par les traitements de données mis en œuvre. Surtout ces règles d'entreprises, pour être contraignantes, doivent faire l'objet d'une approbation pour en garantir leur effectivité. Ainsi, une entreprise souhaitant adopter des règles contraignantes doit d'abord désigner une autorité européenne de protection des données qui sera « chef de file » et qui sera chargée de la procédure de coopération avec les autorités des autres pays européens. Par ailleurs, le principe de cette approbation repose sur la détermination de la responsabilité de l'entreprise adoptant des règles contraignantes. Ainsi, l'entreprise concernée doit mettre en œuvre un régime de responsabilité pesant sur le siège européen responsable de la protection des données ou sur la filiale européenne responsable par délégation de la protection des données et qui acceptent d'endosser la responsabilité pour les actes commis par d'autres filiales en dehors de l'Union européenne[1015].

Créées à l'origine pour des besoins pratiques par les autorités de protection européennes et nationales, ces mesures ont été reprises et consacrées par le RGPD qui exige que ces règles incluent, selon le considérant 110, « tous les principes essentiels et les droits opposables pour assurer des garanties appropriées pour les transferts ou catégories de transferts de données à caractère personnel ». L'article 47 du RGPD, consacré aux règles d'entreprise contraignantes, en précise la portée et les conditions permettant de considérer que ces règles sont juridiquement contraignantes. Surtout, le point j) du texte reprend à son compte la mise en place de mécanismes visant à garantir le contrôle du respect des règles instaurées, notamment à travers des procédures d'audits qui permettent d'assurer que « des mesures correctrices seront prises pour protéger les droits de la personne concernée ».

535. Le contenu des règles. Véritable instrument de conformité à la réglementation, ces règles d'entreprise contraignantes doivent garantir des droits aux personnes concernées par les traitements, qui correspondent aux droits accordés à la

[1015] Anne Debet, Jean Massot, Nathalie Metallinos, *op. cit.*, p. 717.

personne par le RGPD lorsqu'un traitement de données est mis en œuvre : respect du principe de finalité, droit d'accès, de rectification ou encore d'effacement. Celles-ci doivent faire l'objet d'un suivi de la part de l'entreprise concernée, qui doit effectivement indiquer quelles sont les mesures mises en œuvre pour assurer le caractère contraignant des règles édictées. Le point 14 du document de travail établissant un cadre pour la structure des règles d'entreprise contraignantes indique notamment l'engagement que doit prendre la société à effectuer des audits concernant le respect des règles d'entreprise contraignantes au sein du groupe[1016]. Ainsi, les règles contraignantes doivent non seulement être édictées mais l'entreprise concernée doit également être en mesure de démontrer de façon régulière que ces règles sont effectivement respectées. Surtout, le résultat de ces audits « doit permettre aux autorités de protection des données de réaliser elles-mêmes des audits sur la protection des données, si besoin est ».

536. L'extension du mécanisme. Les règles contraignantes ne concernaient jusqu'en 2012 que les transferts effectués au sein d'un groupe agissant en qualité de responsable de traitement. Mais le mécanisme a par la suite été étendu aux sous-traitants, permettant ainsi de « créer une sphère de sécurité pour les transferts effectués au sein d'un groupe agissant en qualité de sous-traitant pour le compte et sur les instructions d'un responsable de traitement »[1017]. A ce titre, cette extension du domaine des règles d'entreprise contraignantes est susceptible de concerner directement les entreprises opérant dans le domaine du *quantified-self*. Il n'est en effet pas rare que de grands groupes, équipementiers sportifs par exemple, développent leurs services d'automesure connectée en ayant parfois recours à des sous-traitants. Le groupe de l'article 29 a d'ailleurs apporté certaines précisions sur cette applicabilité des règles d'entreprise contraignantes aux groupes de sous-traitants dans différents documents explicatifs[1018]. Entre ce recours à un tiers et l'internationalisation des traitements opérés directement par les applications développées, l'instauration de *binding corporate rules* relatives aux sous-traitants est

[1016] G29, *Document de travail établissant un cadre pour la structure des règles d'entreprise contraignantes*, WP 154, 24 juin 2008, p. 8.
[1017] CNIL, *Les BCR (règles internes d'entreprise)*, 6 novembre 2017, accessible en ligne : https://www.cnil.fr/fr/les-bcr-regles-internes-dentreprise
[1018] Voir par exemple : G29, *Document explicatif sur les règles d'entreprise contraignantes applicables aux sous-traitants*, WP 204, 19 avril 2013.

susceptibles d'apporter un degré de protection supplémentaire aux individus utilisant de tels services.

2. Des modalités renouvelées de transfert de données

537. L'alternative à la reconnaissance d'un niveau de protection suffisant. Les encadrements internationaux de transferts de données reposent, à l'origine, sur la reconnaissance du niveau de protection suffisant mis en œuvre par l'Etat destinataire des données à caractère personnel. Cette reconnaissance, qui suppose une appréciation *in concreto* des mesures protectrices mises en œuvre par un Etat tiers, est en théorie de la compétence exclusive de la Commission puisque celle-ci procède à l'adoption de décisions d'adéquation. Les Etats membres disposent certes d'un pouvoir limité d'intervention, en vertu de leur rôle d'information mutuelle permettant des constats provisoires de non-adéquation, mais la Commission reste l'actrice principale de ce mécanisme. Or, ce mécanisme d'adéquation est expressément repris par le RGPD qui indique en son article 45 qu'un « transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat ».

Les *binding corporate rules* visent à « assurer à la personne concernée un niveau de protection équivalent quel que soit l'Etat dans lequel ses données sont effectivement traitées » et permettent dès lors de « couvrir une exception dans la prohibition de principe des transferts de données vers les pays dont le système de protection n'est pas considéré comme adéquat par l'union »[1019]. A l'origine, ces règles ont été instaurées pour constituer « une réponse au défi posé par les transferts internationaux de données » compte tenu notamment de la globalisation des échanges et par une « conformité aux restrictions posées par la législation européenne […] devenue de plus en plus difficile »[1020]. Ainsi, le considérant 107 du Règlement précise que si le constat par la Commission qu'un pays tiers, un territoire ou un secteur

[1019] Nathalie Martial-Braz, Judith Rochfeld, Emilie Gattone, « Quel avenir pour la protection des données à caractère personnel en Europe ? », *Recueil Dalloz*, 2013, p. 2788.

déterminé dans un pays tiers ou une organisation internationale n'assure plus un niveau adéquat de protection des données, le transfert de données vers ce pays tiers ou cette organisation internationale devrait être en théorie interdit, à moins que les exigences du présent règlement relative aux transferts fassent l'objet de garanties appropriées, « y compris des règles d'entreprise contraignantes ». Le considérant 108 précise également que ces règles d'entreprise contraignantes peuvent jouer le rôle de garantie en l'absence de décision d'adéquation et qu'elles constituent, à ce titre, une mesure « pour compenser l'insuffisance de la protection des données dans le pays tiers par des garanties appropriées en faveur de la personne concernée ». La CNIL a par exemple autorisé en 2016, sur le fondement de BCR, le transfert hors espace économique européen des données du groupe Hewlett Packard, rappelant le principe selon lequel un niveau de protection suffisant peut-être apporté par l'intermédiaire de règles internes[1021].

538. Les entreprises souhaitant procéder à des transferts internationaux de données à caractère personnel peuvent donc recourir à des solutions alternatives, en l'absence de décisions d'adéquation. Notamment, deux ou plusieurs sociétés procédant à des transferts internationaux de données peuvent contractualiser des règles adéquates de protection. Autorisées par une autorité de contrôle, ces clauses contractuelles permettent l'instauration de garanties appropriées relatives au traitement et la reconnaissance de « droits opposables et de voies de droits effectives » pour les personnes concernées par le traitement[1022]. Les règles d'entreprise contraignantes visent ainsi à assurer un niveau de protection adéquat aux personnes concernées par des transferts internationaux de données, mais elles reposent pourtant sur un mécanisme de nature et de portée différente. En effet, les *binding corporate rules* ne reposent plus sur une contractualisation de règles protectrices de données à caractère personnel, mais elles permettent à un groupe d'entreprises d'établir directement ces règles.

[1020] Anne Debet, Jean Massot, Nathalie Metallinos, *op. cit*., p. 710.
[1021] Délibération n° 2016-254 du 21 juillet 2016 portant autorisation unique de transferts de données à caractère personnel hors Espace économique européen encadrés par les règles internes d'entreprise (BCR) « responsable de traitement » du groupe Hewlett Packard Enterprise (BCR-033)
[1022] Article 46 du Règlement (UE) 2016/679.

539. L'autonomisation du responsable de traitement. La consécration des BCR, qui existaient déjà avant l'adoption du RGPD, s'inscrit dans le changement de paradigme mis en œuvre par la réglementation. Adoptées sous le contrôle d'autorités administratives européennes, la mise en œuvre de règles d'entreprise contraignantes s'insère dans le mouvement de responsabilisation des différents opérateurs du numérique. Indépendamment de toute décision d'adéquation ou de tout rapport contractuel avec un tiers, un responsable de traitement va directement adopter une réglementation interne protectrice des données à caractère personnel. Cette réglementation sera en théorie une reprise du dispositif protecteur prévu par le Règlement et ses composantes principales, mais le processus tend à illustrer le changement qui est mis en œuvre. En effet, le responsable de traitement dispose désormais d'une certaine autonomie quant à l'instauration d'un dispositif protecteur. Une fois approuvée par les autorités de protection, « les règles internes d'entreprise permettent aux entreprises multinationales de transférer les données personnelles en leur sein sans avoir à rechercher, pour chaque transfert ou catégorie de transfert, s'il existe un fondement légal pour le transfert »[1023].

Cette autonomisation du responsable de traitement semble mieux adaptée à l'émergence et au développement de l'automesure connectée. De nombreuses multinationales développent en effet leurs propres applications et dispositifs de *quantified-self*. Or, la mise en œuvre de ces règles d'entreprise contraignantes doit permettre aux personnes concernées d'avoir une meilleure visibilité de l'usage qui est fait de leurs données à caractère personnel, même si certaines questions restent en suspens, relatives notamment à une réutilisation par un tiers extérieur au groupe.

B. La mise en œuvre d'un principe d'*accountability*

540. L'*accountability* désigne, selon la CNIL, « l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données »[1024]. Ce principe n'est pas une innovation : plusieurs textes, telles que les lignes directrices

[1023] Anne Debet, Jean Massot, Nathalie Metallinos, *op. cit.*, p. 711.
[1024] CNIL, Définition de l'accountability, accessible en ligne à cette adresse : https://www.cnil.fr/fr/definition/accountability

émises par l'OCDE en 1980[1025] ou une norme ISO de 2011 relative à la vie privée mettant en œuvre une obligation de diligence couplée à l'adoption de mesures concrètes de protection[1026], y faisaient déjà référence. Surtout, les responsables de traitement avaient déjà l'obligation, sous l'empire de la loi de 1978 modifiée, de se conformer aux dispositions législatives régissant la protection des données à caractère personnel.

L'évolution proposée par le RGPD se distingue par le fait que l'*accountability* irrigue un nombre important de règles mises en œuvre. Ce principe impose en effet au responsable de traitement d'être en mesure de prouver, à tout moment, qu'il respecte l'ensemble des règles de protection. Ainsi, l'*accountability* permet de repenser les modalités de mise en œuvre des traitements de données à caractère personnel **(1)**, modalités dont le respect est également assuré par la désignation d'un délégué à la protection des données à caractère personnel **(2)**.

1. Des modalités de traitement repensées

541. Le RGPD a introduit un nouveau paradigme fondé sur l'*accountability*. Celui-ci vise à imposer au responsable de traitement l'adoption de mesures technologiques et organisationnelles pour se conformer au règlement et être en mesure de prouver cette mise en conformité. A ce titre, le rôle du responsable de traitement est d'apprécier, « compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques »[1027], les mesures les plus appropriées pour préserver les droits et les libertés des personnes concernées par le traitement. La traduction du terme d'*accountability*, se référant uniquement à la responsabilité, est incomplète et ne reflète pas toute la signification de ce terme[1028]. En effet, l'article 24 du RGPD traitant de la responsabilité du responsable de traitement indique que celui-

[1025] Celles-ci disposent notamment que « tout maître de fichier devrait être responsable du respect des mesures donnant effets aux principes matériels énoncés ci-dessous ».
[1026] ISO/IEC 29100 :2011, Information technology - Security techniques - Privacy framework.
[1027] Éléonore Scaramozzino, « Open data versus protection des données : les enjeux pour le tourisme des smart cities », *Juris Tourisme*, 2018, n°207, p. 24.
[1028] Nathalie Metallinos, « 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 ; Anne Debet, « Les nouveaux instruments de conformité », *Dalloz IP/IT*, 2016, p. 592 ; Florence Bonnet, « Règlement Européen de Protection des Données personnelles : le principe d'accountability ou comment passer de la théorie à la pratique », *CIL Consulting*, 18 mars 2017, Winston Maxwell, Célia Zolynski, « Protection des données personnelles », *Recueil Dalloz*, 2019, p. 1673.

ci doit mettre en œuvre « des mesures techniques et organisationnelles appropriées » au regard des risques que le traitement est susceptible de présenter pour les droits et libertés des personnes physiques. Mais surtout, celui-ci doit « être en mesure de démontrer » que le traitement est effectué conformément au règlement. Ainsi, le responsable de traitement n'est pas seulement responsable du respect des principes fondamentaux de la réglementation tels que ceux relatifs au respect du principe de finalité, à la licéité du traitement, à sa loyauté ou encore sa transparence. Encore faut-il qu'il soit en mesure de prouver la bonne exécution du dispositif protecteur établi.

Dès 2010, le G29 proposait « la mise en œuvre de mesures et procédures internes en vue d'appliquer les principes existants de protection des données et de garantir leur efficacité, ainsi que l'obligation de le démontrer à la demande des autorités chargées de la protection des données »[1029], pour encourager les responsables du traitement des données à prendre des mesures offrant une réelle protection. La consécration d'un tel dispositif permet une meilleure prise en compte de la croissance du nombre de données à caractère personnel générées, traitées et transférées, favorisée notamment par l'évolution technologique, la multiplication des systèmes d'information et de communication ainsi que par la capacité grandissante des personnes à utiliser les technologies et à interagir avec celles-ci[1030]. Le *quantified-self* cristallise, par les objets et applications utilisés ainsi que par l'automatisation des modalités de collecte, cette évolution. Le développement de l'*accountability* serait dès lors susceptible de mieux encadrer les traitements réalisés dans ce cadre.

542. La délégation de certains pouvoirs normatifs. Le principe d'*accountability* est aujourd'hui révélateur d'une évolution plus générale du mécanisme protecteur des données à caractère personnel. L'*accountability*, au même titre que le mécanisme mis en place par les *binding corporate rules*, marque en effet « la délégation par le régulateur de certains pouvoirs normatifs »[1031]. Outil de co-régulation, l'*accountability* illustre la décentralisation du pouvoir normatif étatique en

[1029] G29, *Avis n° 3/2010 sur le principe de la responsabilité*, WP 173, adopté le 13 juillet 2010, p. 6.
[1030] *Ibid.*, p. 5.
[1031] Winston Maxwell, Sarah Taïeb, « L'accountability, symbole d'une influence américaine sur le règlement européen des données personnelles ? », *Dalloz IP/IT*, 2016, p. 123.

matière de protection des données à caractère personnel. Les responsables de traitement, eux-mêmes chargés d'assurer la protection des données qu'ils traitent, deviennent en effet co-régulateurs du dispositif protecteur par la mise en place de programmes de conformité. L'article 24, alinéa 2 du RGPD indique à ce titre que « lorsque cela est proportionné au regard des activités de traitement, les mesures […] comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement ». Outre le cadre réglementaire mis en place, les responsables de traitement sont ainsi invités à mettre directement en place des mesures qui permettent de protéger les données dont ils ont la responsabilité.

543. La personnalisation de la protection. Enfin, le principe d'*accountability* justifie l'abandon des formalités déclaratives préalables. La lourdeur administrative du procédé mis en œuvre, les incertitudes entourant les conditions de déclaration ou encore les éventuelles dispenses sont remplacées par le rôle actif conféré au responsable du traitement qui va venir se substituer au régulateur pour la mise au point de règles internes. On constate ainsi l'établissement « d'une norme « sur-mesure » qui définit un cadre à respecter prenant en compte le plus possible le contexte, les activités et les contraintes pour l'entreprise concernée »[1032]. Ainsi, outre cette décentralisation du pouvoir normatif au cœur de l'entreprise traitant des données à caractère personnel, ce renouvellement de la réglementation permet une personnalisation de la protection en fonction de chaque traitement réalisé.

Certaines des problématiques issues du *quantified-self* auraient ainsi tendance à s'effacer. Par exemple, les hésitations sur le régime juridique à apporter aux données traitées – donnée personnelle, donnée sensible, donnée de santé, conclusions relatives à l'état de santé – importeraient moins. D'une part, une protection « sur mesure » sera apportée aux informations collectées et traitées, en fonction de leurs spécificités et d'autre part, les responsables de traitement auront l'obligation, à tout moment, de démontrer qu'ils agissent en conformité avec la réglementation et donc qu'ils protègent efficacement ces données. Dès lors, plutôt qu'un cadre juridique de portée générale, le développement d'une protection fondée sur la conformité est susceptible d'assurer une meilleure prise en compte des particularités de chacun des

traitements mis en œuvre, en fonction des entreprises qui en sont responsables. L'établissement du principe d'*accountability* ne représente par ailleurs pas une fin en soi, car il justifie le déploiement de certaines mesures par le responsable de traitement, à l'image de l'obligation qui lui est faite de tenir des registres des activités de traitement en vertu de l'article 30 du RGPD.

544. Le renversement de la charge de la preuve. Le règlement offre un certain pouvoir de modulation aux responsables de traitement, susceptibles d'adapter les règles applicables en fonction de leurs processus de collecte. Cette adaptation du cadre juridique protecteur est également susceptible de s'accompagner d'un renversement de la charge de la preuve. Les autorités de contrôle et personnes concernées par le traitement devaient à l'origine apporter la preuve du manquement à la réglementation par le responsable de traitement. Ce dernier est désormais tenu de fournir la preuve de l'exécution du traitement conformément à la réglementation. Par ailleurs, même si le principe d'*accountability* ne semble pas concerner directement le sous-traitant en ce qu'aucune disposition ne lui impose de montrer qu'il agit conformément à la réglementation, celui-ci doit pourtant également présenter « des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées », selon l'article 28 du RGPD. L'instauration d'un principe d'*accountability*, censé assurer un degré de protection supplémentaire en amont, ne préjuge pas de cette conformité et d'éventuelles sanctions ultérieures[1033]. Mais celui-ci permet de justifier du renforcement du rôle du délégué à la protection des données à caractère personnel.

2. Des modalités de traitement protégées

545. La désignation d'un délégué à la protection des données. L'application du principe d'*accountability* s'accompagne de la publication, par les autorités

---

[1032] *Ibid*.

[1033] Le groupe de l'article 29 précise en ce sens, dans l'avis WP 173 adopté le 13 juillet 2010, que « l'adoption, par un responsable du traitement des données, de mesures destinées à observer les principes ne doit en aucun cas exclure la mise en œuvre à son encontre de mesures coercitives lorsque les autorités chargées de la protection des données l'estiment nécessaire ».

nationales de protection, de packs de conformité à destination des responsables de traitement. Or, un relais supplémentaire est assuré, au sein des entreprises elles-mêmes, par la désignation d'un délégué à la protection des données à caractère personnel qui, « peu importe qu'ils soient ou non des employés du responsable du traitement, devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance »[1034]. Ainsi, le RGPD impose au responsable de traitement des données, opérateurs privés, de désigner un délégué à la protection des données personnelles lorsque « les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées »[1035].

Le G29 a eu l'occasion de préciser, dans ses lignes directrices relatives aux délégués à la protection des données, que le terme « régulier » employé s'entend d'un traitement qui est en cours, récurrent, constant ou se produisant à intervalles réguliers, contrairement au terme « systématique » qui vise lui le suivi dans le cadre d'un plan général de collecte de données[1036]. Par ailleurs, l'article 37 du texte européen précise en son point 1. c) qu'un délégué à la protection des données doit être désigné lorsque « les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 » et qui porte donc sur des données sensibles.

546. L'adéquation des critères au *quantified-self*. Au regard des critères développés par le groupe de l'article 29, la désignation d'un délégué à la protection des données à caractère personnel devrait être obligatoire pour les entreprises en charge du développement de services de *quantified-self* ou d'objets connectés utilisés dans ce but. En effet, les modalités de collecte qui sont mises en œuvre par ces services répondent en théorie aux critères de désignation établis par le G29 pour l'interprétation des termes du Règlement[1037]. Il semble difficile de déterminer

[1034] Considérant 97 du Règlement (UE) 2016/ 679.
[1035] *Ibid.*, article 37.
[1036] G 29, Lignes directrices sur le délégué à la protection des données, WP 243, 13 décembre 2016, p. 7.
[1037] Celui-ci ne donne pas de définition précise du traitement réalisé à grande échelle mais précise seulement au sein du considérant 91 que ceux-ci « visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé, par exemple, en raison de leur caractère sensible ».

précisément ce qui constitue un traitement « à grande échelle », mais le facteur relatif au nombre de personnes concernées par le traitement pourrait servir d'indicateur pour déterminer son spectre. Ainsi, une application téléchargée un très grand nombre de fois devrait donc, conformément aux critères mis en œuvre par le G29, être révélatrice d'un traitement réalisé à grande échelle, d'autant que celles-ci ne sont pas limitées géographiquement quant à leurs téléchargements et qu'elles sont donc susceptibles de toucher des zones territoriales élargies. A titre d'exemple, les applications de *running* Runtastic, Nike+ Run Club et Runkeeper comptabilisent plusieurs millions de téléchargements rien que pour le magasin d'application en ligne Google Play. Le fait que ces applications aient été téléchargées autant de fois doit permettre de considérer qu'un traitement est réalisé à grande échelle.

Par ailleurs, au regard de l'absence de définition du traitement dit « régulier »[1038] et de son interprétation par le groupe de l'article 29, un objet connecté ou une application procédant à des mesures à intervalles réguliers ou même constantes correspond sans nul doute à un traitement régulier de données justifiant la désignation d'un délégué à la protection des données à caractère personnel ; le G29 mentionne d'ailleurs expressément la surveillance d'éléments relatifs au bien-être ou à la santé par des *trackers* d'activité comme constituant un traitement régulier[1039]. La désignation d'un délégué à la protection sera *a fortiori* obligatoire si l'on considère que les traitements mis en œuvre dans le cadre du *quantified-self* portent sur des données de santé et donc sur des catégories particulières de données visées à l'article 9 du Règlement.

547. Le garant du principe d'*accountability*. Le délégué à la protection des données personnelles, successeur du correspondant Informatique et Libertés et recruté sur la base de ses compétences[1040], a vocation à devenir le garant du principe d'*accountability* déterminé par le Règlement européen. Le considérant 77 du texte précise explicitement que le délégué à la protection des données peut donner des indications au responsable de traitement ou au sous-traitant quant à la « mise en

[1038] Le considérant 24 du Règlement fait simplement référence au « suivi du comportement des personnes concernées », critère vérifié si les « personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique ».
[1039] G29, WP 243, *op. cit.*, p. 9.

œuvre de mesures appropriées et à la démonstration […] du présent règlement ». En tout état de cause, le responsable de traitement doit faciliter l'identification du délégué à la protection des données personnelles et fournir cette information à la personne concernée au moment de la collecte des données.

Le délégué à la protection des données est de manière plus générale associé « à toutes les questions relatives à la protection des données à caractère personnel » selon l'article 38 du texte. Doté d'une mission d'information à l'égard du responsable du traitement ou du sous-traitant, chargé de contrôler directement le respect des règles relatives à la protection des données, il fait également office de point de contact avec l'autorité de contrôle, étant donné qu'il coopère avec celle-ci. Par ailleurs, il est en charge de contrôler le respect des règles internes mises en œuvre, ce qui lui permet de s'affirmer comme un garant du principe d'*accountability* et de sa bonne exécution dans le cadre de la décentralisation du dispositif protecteur. Certaines de ses fonctions étaient déjà connues sous l'empire de la loi Informatique et Libertés mais l'expansion de ses champs de compétence au sein du RGPD permet de lui attribuer un rôle harmonisé[1041].

548. La place nouvelle qui est conférée au délégué à la protection des données permet d'apporter certaines garanties supplémentaires aux traitements réalisés pour la pratique de l'automesure. D'abord, l'étendue des traitements réalisés dans ce cadre devrait conduire à la désignation systématique d'un délégué à la protection des données. Ensuite, l'indépendance du DPO doit lui permettre d'exercer des contrôles supplémentaires, contrôles que le responsable de traitement pourrait être réticent à mettre en œuvre étant donné la quantité d'informations collectées dans le cadre du *quantified-self*. Enfin, la présence du délégué constitue, au vu de la sensibilité des informations traitées, une garantie supplémentaire pour la personne concernée par un traitement d'automesure. Le DPO est en effet associé à la mise en œuvre des différentes mesures relatives à l'*accountability*, entre notifications des failles de

[1040] Virginie Langlet, « Nom de code : délégué à la protection des données », *Juris Tourisme*, 2018, n°207, p.29.
[1041] Andrea Carrera Mariscal, « Le CIL : modèle type du futur délégué à la protection des données ? », *Dalloz IP/IT*, 2018, p. 233.

sécurité et développement d'études d'impact relatives à la vie privée, éléments qui permettent de garantir la transparence des opérations de traitement réalisées.

§2. La confirmation d'une obligation de transparence

549. Le changement de paradigme opéré par la réglementation renouvelée vise au respect d'une obligation de conformité des responsables de traitement aux règles protectrices des données à caractère personnel. Mais celle-ci s'insère plus généralement dans le cadre d'une obligation de transparence qui pèse sur les responsables de traitement. Prolongement de l'obligation de loyauté, cette transparence doit garantir une autodétermination informationnelle aux personnes concernées en leur donnant une visibilité sur les opérations réalisées à partir de leurs informations nominatives. Cette transparence justifie qu'une information claire soit délivrée aux personnes concernées par des traitement[1042]. Elle va pourtant plus loin en favorisant la mise en place de certaines mesures complémentaires[1043]. Parmi celles-ci, le développement des analyses d'impact sur la vie privée **(A)** ainsi que les notifications des failles de sécurité **(B)** participent efficacement de cette obligation générale de transparence.

A. Le développement des analyses d'impact sur la protection des données

550. L'article 35 du RGPD marque l'introduction dans la règlementation d'une analyse d'impact relative à la protection des données à caractère personnel. Celle-ci, effectuée par le responsable avant la mise en place du traitement, vise à mesurer les conséquences du traitement lorsque celui-ci, « compte tenu de la nature, de la portée, du contexte et des finalités […], est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ». Cette analyse d'impact relative à la protection des données conforte la mise en place d'une protection *ex ante* **(1)** dont la portée s'avère toutefois limitée **(2)**.

[1042] Le considérant 39 du Règlement précise en ce sens que « le principe de transparence exige que toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples ».
[1043] Le considérant 100 du Règlement suggère la mise en place de mécanismes de certification ainsi que de labels et de marques afin de favoriser la transparence et le respect du Règlement.

1. Une protection *ex ante*

551. Les règles relatives à la protection des données à caractère personnel sont progressivement décentralisées et font des opérateurs du numérique, des co-régulateurs de la protection des données traitées. La temporalité de cette régulation est également en plein changement puisqu'une régulation *ex ante* et préventive est aujourd'hui développée au profit d'une régulation qui était antérieurement *ex post* et corrective. Ce changement de paradigme, acté par l'adoption d'un modèle fondé sur la conformité, s'accompagne de mesures concrètes visant à anticiper les risques susceptibles de naître à la suite de tels traitements. Comme le relèvent certains auteurs, « l'analyse d'impact devrait être une procédure plus efficace et plus ciblée que l'obligation générale de notifier les traitements aux autorités de contrôle prévue par la directive n° 95/46/CE »[1044]. Le considérant 89 du RGPD indique à ce titre que la procédure mise en œuvre par la directive « génère une charge administrative et financière, sans pour autant avoir systématiquement contribué à améliorer la protection des données à caractère personnel », ce qui justifie dès lors sa suppression au profit de « procédures » et de « mécanismes efficaces ciblant plutôt les types d'opérations de traitement susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, du fait de leur nature, de leur portée, de leur contexte et de leurs finalités ».

552. Le risque pour les libertés. L'analyse d'impact repose, pour sa mise en œuvre, sur l'appréciation de la portée du traitement, « susceptible d'engendrer un risque élevé » pour les droits et libertés des personnes physiques. Également entendu comme une « analyse d'impact sur la vie privée », celle-ci s'insère de manière plus générale sur l'appréciation de la conformité aux règles du RGPD. Ces analyses représentent également un « outil important au regard du principe de responsabilité, compte tenu de leur utilité pour les responsables du traitement non seulement aux fins du respect des exigences du RGPD, mais également en ce qui concerne leur capacité à démontrer que des mesures appropriées ont été prises pour assurer la conformité au

[1044] Ioana Gheorghe-Badescu, « Le nouveau règlement général sur la protection des données », *Revue de l'Union européenne*, 2016, p. 466.

règlement »[1045]. Le risque présenté à l'article 35 du Règlement porte sur les « droits et libertés des personnes physiques » et vise prioritairement le droit à la protection des données et à la vie privée. Mais le G29, attestant de la portée élargie attribuée à ce mécanisme, considère que celui-ci doit être étendu à d'autres droits fondamentaux, tels que « la liberté de parole, la liberté de pensée, la liberté de circulation, l'interdiction de toute discrimination, le droit à la liberté ainsi que la liberté de conscience et de religion »[1046]. Par ailleurs, outre l'appréciation d'une opération unique de traitement, cette analyse peut également être utilisée pour évaluer plusieurs opérations de traitement similaires.

Comme le relève le groupe de l'article 29, l'analyse d'impact n'est pas nécessaire pour apprécier tout type de risques pour les droits et libertés des personnes physiques mais uniquement pour les traitements susceptibles d'engendrer un risque « élevé ». Trois types de traitement susceptibles de présenter ce risque sont ainsi présentés à l'article 35 du texte[1047] sans que l'on puisse pour autant considérer que cette énumération soit exhaustive[1048].

553. Plusieurs critères d'application sont retenus pour considérer qu'un traitement de données doit faire l'objet d'une analyse d'impact, dont certains doivent être appliqués au domaine des objets connectés et du *quantified-self*. Sont particulièrement concernés les traitements susceptibles de mettre en œuvre une « évaluation ou notation » des personnes concernées, ceux relatifs à la « surveillance systématique » ou encore ceux relatifs aux « données sensibles ou données à caractère hautement personnel ». Ces critères sont applicables aux données traitées, que celles-ci soient « traitées à grande échelle » ou que celles-ci fassent l'objet d'un « croisement ou d'une combinaison ». Le *quantified-self*, par les objets ou applications utilisés, est susceptible de remplir chacun de ces critères et permettrait

---

[1045] G 29, *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*, p. 4.
[1046] *Ibid.*, p. 7.
[1047] « L'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ; le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ; ou la surveillance systématique à grande échelle d'une zone accessible au public ».
[1048] G29, *op. cit.*, p. 10.

également de porter atteinte à chacun des droits fondamentaux précités. Les données de géolocalisation relevées par un *tracker* d'activité, révélant qu'un individu se rend régulièrement au siège d'un parti politique, pourraient être utilisées pour entraver la liberté de circulation ou porter atteinte à la liberté de pensée ou de conscience. Les données d'une application de régime alimentaire, en révélant une liste d'aliments proscrits, pourraient permettre de porter atteinte à la liberté de religion. Enfin, les données relatives à l'activité physique, révélatrices de certains handicaps, seraient susceptible d'être une source de discrimination. Le G29 fait ainsi directement référence à « certaines applications de l'Internet des objets » qui « sont susceptibles d'avoir un impact important sur la vie quotidienne et la vie privée des personnes » et un guide relatif à l'analyse d'impact portant sur les objets connectés a d'ailleurs été publié par la CNIL[1049].

554. La maîtrise du risque. La mise en œuvre d'une analyse d'impact, au regard des critères évoqués, vise à garantir aux individus une maîtrise des risques susceptibles de se réaliser lorsqu'un traitement est mis en œuvre. Outil de responsabilisation des responsables de traitement, cette analyse s'inscrit dans une démarche de conformité puisque celle-ci doit contenir, selon l'article 35 du Règlement, « les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement ». Plus qu'une simple identification des risques, celle-ci doit conduire à la mise en œuvre d'un dispositif concret de maîtrise du risque.

La description du traitement mis en oeuvre, eu égard notamment à la finalité, à la nécessité et la proportionnalité des opérations réalisées, doit permettre de déterminer en amont les réponses à apporter par le responsable du traitement afin d'agir en conformité avec les règles protectrices du RGPD. Surtout, cette maîtrise préventive est réalisée sous le contrôle d'une autorité de contrôle. En effet, en vertu de l'article 36 du Règlement, lorsqu'une analyse d'impact révèle la présence d'un risque pour les personnes concernées, le responsable du traitement doit consulter celle-ci si, en l'absence de mesures prises pour atténuer le risque, le traitement est

[1049] CNIL, *PIA, Applications aux objets connectés*, février 2018, 50 p.

tout de même mis en œuvre. Ainsi, ce mécanisme vise à assurer la transparence du traitement mis en œuvre quant aux risques potentiels. Son efficacité semble cependant limitée.

2. Un mécanisme protecteur limité en pratique

555. L'analyse d'impact relative à la protection des données à caractère personnel n'est pas un mécanisme nouveau[1050]. Pourtant, « sa capacité d'améliorer effectivement la protection de ces données reste encore à évaluer après 2018 »[1051]. L'instauration d'une analyse d'impact vise à favoriser concrètement la protection en amont des personnes concernées par le traitement. Pourtant, les modalités de mise en œuvre d'une telle analyse ne semblent pas constituer un rempart infranchissable au risque informationnel pesant sur les individus. La mise en œuvre d'une analyse d'impact, bien que permettant de répondre à l'exigence de protection des données dès la conception, n'est, en effet, pas obligatoire. Certains traitements courants devraient en effet pouvoir échapper à ce mécanisme et l'obligation de réaliser une analyse d'impact est laissée à l'appréciation subjective du responsable de traitement. De plus, si le responsable de traitement reste *in fine* responsable de la mise en œuvre de cette analyse[1052], celle-ci peut également être effectuée par une tierce personne.

Délégué à la protection des données et sous-traitant sont dans certains cas associés à cette analyse, afin de contribuer à la conformité du traitement aux nouvelles règles européennes. Par exemple, lorsqu'un délégué à la protection des données est désigné, le responsable du traitement est tenu de prendre conseil auprès de lui. Ce dernier les dispense « sur demande » et veille à l'exécution de l'analyse d'impact en vertu de l'article 39 du RGPD. Lorsque le traitement est réalisé en tout ou partie par un sous-traitant, ce dernier doit aider le responsable du traitement à réaliser cette analyse en lui transmettant les informations nécessaires. Mais, malgré l'aide de ces différentes parties[1053], le responsable du traitement endosse l'entière responsabilité de l'analyse d'impact. Aussi, en l'absence de mécanisme de déclaration

[1050] La CNIL a publié des guides relatifs à la mise en œuvre d'analyse d'impact dès 2015.
[1051] Ioana Gheorghe-Badescu, art. précité., p. 468.
[1052] G29, *op. cit*., p. 17.

préalable du traitement à une autorité externe à l'entreprise, la mise en œuvre effective d'une analyse d'impact ne fait l'objet d'aucun contrôle *a priori*. L'importance des sanctions est susceptible de dissuader les responsables de traitement de ne pas procéder à une telle analyse[1054], mais il n'existe aucune garantie permettant d'assurer que celle-ci sera réalisée. Sa publication n'est d'ailleurs pas rendue obligatoire par le RGPD même si elle peut, selon la CNIL, faire l'objet d'un rapport ou d'un résumé pouvant être communiqué et s'inscrire dans le cadre des bonnes pratiques améliorant la confiance[1055].

556. Autre facteur d'incertitude, la définition du « risque élevé » est susceptible de connaître de « nombreuses définitions, parfois très différentes en fonction du secteur d'activité concerné »[1056]. Impossible à définir par avance de manière exhaustive, l'absence de précision concrète de cette notion est susceptible d'engendrer des divergences d'appréciation en fonction des différents responsables de traitement. Les autorités de contrôle nationales doivent établir et publier une liste « des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise »[1057]. Mais, le caractère non-limitatif des termes employés ainsi que l'appréciation élargie qui en est faite, par le G29 notamment, est susceptible de compliquer la mise en œuvre de cette analyse.

L'analyse d'impact ne permet donc pas une prévention absolue des risques. Elle s'insère néanmoins dans un dispositif protecteur plus large qui, tout en instaurant des mesures de protection dès la conception, conserve certains éléments de réglementation *ex post*, tels que les notifications de failles de sécurité.

[1053] L'article 35 paragraphe 9 précise par ailleurs que le responsable du traitement « demande l'avis des personnes concernées ou de leurs représentants ».
[1054] Le montant des amendes peut s'élever jusqu'à 10 000 000 d'euros ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu (article 83, 4, a).
[1055] CNIL, délibération n° 2018-326 du 11 octobre 2018 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le règlement général sur la protection des données (RGPD).
[1056] Académie des sciences et techniques comptables et financières, *Gouvernance des données personnelles et analyse d'impact*, Cahier n°28, octobre 2014, p. 20.
[1057] Article 39, 4 du Règlement (UE) 2016/679.

B. Les notifications des failles de sécurité

557. La prise en compte d'éléments relatifs à la sécurité des traitements de données mis en œuvre n'est pas une nouveauté instaurée par le RGPD. La multiplication des risques liés à la cybercriminalité et aux pertes de données accidentelles a justifié la prise en compte de ce phénomène au sein de la loi Informatique et Libertés modifiée en 2004, celle-ci établissant, avant même sa réécriture, un principe de sécurité et de confidentialité des traitements[1058]. Le non-respect de cette obligation de sécurité, reprise notamment à l'article 99 de la nouvelle loi, est puni par l'article 226-17 du Code pénal d'une peine de cinq ans d'emprisonnement et de 300 000 euros d'amende. Cette obligation de confidentialité et de sécurité des données a un caractère préventif et celle-ci se double d'une obligation de notification des failles de sécurité. Le RGPD précise et élargit en effet cette obligation de notifier les failles de sécurité **(1)**, révélant par la même occasion la survivance d'éléments de réglementation *a posteriori* **(2)**.

1. Un enjeu de transparence

558. Une obligation limitée. Le mécanisme de notification des failles de sécurité mis en œuvre par la loi Informatique et Libertés de 1978 limitait le nombre de personnes débitrices de l'obligation de notification aux « fournisseurs de services de communications électroniques accessibles au public ». Disposition introduite par l'ordonnance n°2011-2012 du 24 août 2011 qui transposait en droit interne l'article 2 de la directive n° 2009/136/CE, cette obligation ne s'appliquait pas à l'ensemble des responsables de traitement, même si ceux-ci étaient tenus de veiller à la sécurité des données traitées et de prendre toutes précautions utiles pour y parvenir[1059]. Les responsables de traitement opérant dans le domaine des objets connectés et du *quantified-self* n'étaient donc pas débiteurs de cette obligation, bien que leur

[1058] L'article 34 de la loi de 1978 indiquait par exemple que « le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données », dispositions auxquels le sous-traitant était également soumis puisqu'il devait, en vertu de l'article 35, « présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34 ».

[1059] G 29, *Avis 03/2014 sur la notification des violations de données à caractère personnel*, 693/14/FR, WP 213, adopté le 25 mars 2014.

assimilation à des prestataires de la société de l'information ait pu être soulevée[1060]. Un règlement datant de 2013 est par la suite venu harmoniser le cadre juridique relatif à cette notification, sans pour autant en élargir la portée puisque pris en vertu de la directive 2002/58/CE traitant spécifiquement des services de communications électroniques accessibles au public[1061]. Le système mis en œuvre reposait sur une double notification, à l'égard de la CNIL et de la personne affectée par la violation, lorsqu'une atteinte était portée aux données à caractère personnel ou à la vie privée de l'intéressé ; la gravité de la violation étant notamment appréciée au regard de la question de savoir si des données sensibles étaient concernées[1062].

559. Une obligation généralisée. Le RGPD modifie le régime de notification mis en place en généralisant l'obligation de notifier une violation de données à caractère personnel à l'ensemble des responsables de traitement[1063]. Le délai de la notification est revu puisqu'elle doit avoir lieu dans les « meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance ». Une exception est mise en place par le texte, qui prend en compte le fait que « la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques ». A l'image du système précédemment en vigueur, la notification est double lorsque la violation de données est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique. Le responsable de traitement doit, sauf s'il a mis en œuvre des mesures de protection techniques et organisationnelles appropriées ou que le risque n'est plus susceptible de se matérialiser, notifier la violation de données à caractère personnel à l'individu. Une autre exception est avancée : le responsable de traitement est dispensé de son obligation de notifier lorsque cette notification entraîne le déploiement d'efforts disproportionnés. Cette exception est aisément compréhensible au regard de l'ampleur des violations de

[1060] ARCEP, *Etude sur le périmètre de la notion d'opérateur de communications électroniques*, Etude réalisée par les cabinets Hogan Lovells et Analysys Mason pour le compte de l'ARCEP, Les actes de l'ARCEP, juin 2011, p. 49.
[1061] Règlement (UE) n° 611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques.
[1062] *Ibid.*, article 3. 2. a) qui indique qu'il est « déterminé si une violation de données à caractère personnel est susceptible de porter atteinte aux données à caractère personnel ou à la vie privée » au regard notamment des « catégories de données particulières visées à l'article 8, paragraphe 1, de la directive 95/46/CE ».
[1063] L'article 33 du Règlement précise ainsi qu'en « cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente ».

données qui peuvent être réalisées et du nombre de personnes susceptibles d'être concernées par de telles violations.

560. La généralisation de cette obligation de notifier les failles de sécurité relatives aux traitements s'inscrit dans le mouvement global de transparence sous-tendant le RGPD. La généralisation de la notification des failles de sécurité ne concerne pas directement la décentralisation du pouvoir régulateur, mais elle permet d'autonomiser les responsables de traitement à l'égard de l'autorité de contrôle et également des personnes concernées par la violation de données à caractère personnel. Dans la notification, les responsables doivent être en mesure de décrire quelles mesures ont été prises pour remédier à la violation de données, au regard de ses conséquences probables. La notification n'empêche pas que d'éventuelles sanctions soient prises à l'encontre du responsable de traitement, surtout lorsqu'il apparaît que les mesures nécessaires pour assurer la sécurité du traitement n'ont pas été mises en œuvre[1064].

561. Le suivi des failles sur la chaîne de traitement. La principale novation du texte, cependant, est d'assurer un suivi de ces violations sur l'ensemble de la chaîne de traitement mise en œuvre. Selon l'article 35.2 du Règlement, le « sous-traitant » notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance. Cette disposition ne semble pas dispenser le responsable du traitement de son obligation de notifier la violation. Mais elle assure une transparence accrue, reposant sur la prise en compte de l'ensemble des acteurs appelés à traiter des données à caractère personnel. Une telle mesure semble particulièrement adaptée aux traitements mis en œuvre dans le cadre du *quantified-self*, en raison des nombreux acteurs qui sont appelés à traiter les mêmes données à caractère personnel. L'article 35.2 du RGPD ne permet donc pas d'œuvrer directement pour la maîtrise du risque informationnel, mais il contribue, par la généralisation des notifications à effectuer, à en limiter les effets en cas de violation des données.

[1064] Nathalie Metallinos, « Notification des violations de données à la CNIL : tendre le bâton pour se faire battre ? », *Dalloz IP/IT*, 2016, p. 144.

Cette obligation de notification renouvelée, survivance d'éléments de réglementation *ex post*, est justifiée par l'impossibilité d'empêcher en amont toute violation de données à caractère personnel.

2. Une survivance d'éléments de réglementation *ex post*

562. Les risques favorisés par le *quantified-self*. La généralisation des notifications des failles de sécurité et de violation des données à caractère personnel s'inscrit dans une logique de responsabilité, de conformité et d'autonomisation des responsables de traitement. Celle-ci est également motivée par le constat de l'impossibilité à maîtriser entièrement et de manière préventive d'éventuels risques pour les données à caractère personnel. La multiplication des attaques informatiques, entre vulnérabilité des traitements mis en œuvre et négligences éventuelles de la part des responsables de traitement, s'accompagne généralement de l'accroissement du nombre de personnes touchées par ces mêmes attaques. En effet, les traitements qui sont réalisés par un même responsable sont de plus en plus importants et permettent dans certains cas la concentration des données traitées, amplifiant dès lors la portée des attaques ou éventuelles négligences. Le domaine du *quantified-self* et des objets connectés est à ce titre particulièrement touché puisqu'il permet la mise en œuvre de traitements d'ampleur, généralisé par le recours à des applications souvent gratuites. L'automatisation des procédés de collecte étant facilitée, un nombre important de données est susceptible de faire l'objet de malveillances.

563. Le piratage. A titre d'exemple, l'application *My Fitness Pal* permettant de compter le nombre de calories ingérées quotidiennement a fait l'objet d'un piratage massif en février 2018, affectant près de 150 millions d'utilisateurs et compromettant leurs adresses de courrier électronique, identifiants et mots de passe[1065]. Ce piratage ne concernait pas directement les données à caractère personnel d'automesure mais son ampleur est révélatrice des risques particuliers pesant sur le *quantified-self*. Plusieurs études réalisées ont déjà eu l'occasion de montrer qu'il s'agit d'un domaine particulièrement sensible en raison du nombre de données

collectées et du nombre de personnes potentiellement touchées[1066]. D'autant que les objets et applications utilisés dans le cadre de l'automesure ne sont généralement pas développés en prenant en compte des paramètres relatifs à la sécurité, ce qui les rend particulièrement perméables à des attaques informatiques[1067]. Les données collectées deviennent ainsi plus facilement accessibles aux tiers qui peuvent éventuellement en faire une utilisation malveillante. Par ailleurs, les capacités d'interconnexion des différents outils utilisés dans le cadre de l'automesure connectée (application, *smartphone*, tablette, ordinateur) et les possibilités d'association de différents comptes personnels font qu'une vulnérabilité est susceptible d'impacter l'ensemble des dispositifs et des comptes utilisés par l'utilisateur.

564. Le défaut de sécurisation des objets. Les failles de sécurité présentées par les objets connectés sont aujourd'hui facilement identifiables. Il existe par exemple un moteur de recherche, « shodan.io », qui permet de détecter les objets connectés vulnérables et exposés à des risques informatiques. Les questions relatives au piratage ne sont pas propres au *quantified-self*[1068] mais celui-ci permet, au regard de la sensibilité des informations collectées, de mesurer l'ampleur des risques associés à un défaut de sécurisation des dispositifs étant donné que près de 80% d'entre eux ne font l'objet d'aucune mesure de sécurité[1069]. Ces risques sont renouvelés par les capacités de ces objets à dialoguer entre eux et à s'échanger directement et sans intermédiaires des informations nominatives et identifiantes[1070]. La croissance exponentielle du nombre de piratages, le manque de sensibilisation des différents acteurs impliqués et les spécificités techniques propres aux objets connectés font que l'emploi de cette nouvelle technologie, parfois mal appréhendée, constitue en lui-même un risque supplémentaire pour les individus. L'absence de

---

[1065] The Guardian, *Hackers steal data of 150 million MyFitnessPal app users*, 30 March 2018, accessible en ligne à cette adresse : https://www.theguardian.com/technology/2018/mar/30/hackers-steal-data-150m-myfitnesspal-app-users-under-armour

[1066] Mario Ballano Barcena, Candid Wueest, Hon Lau, *How safe is your quantified self*, Symantec, August 11, 2014.

[1067] Marie-Helen Maras, « Internet of Things : security and privacy implications », *International Data Privacy Law*, Oxford University Press, April 7, 2015.

[1068] Voir par exemple le piratage du site de rencontres Ashley Madison ayant touché près de 33 millions d'utilisateurs : http://www.lemonde.fr/pixels/article/2015/08/20/piratage-d-ashley-madison-qui-sont-les-victimes_4731634_4408996.html

[1069] Gérard Haas, Amanda Dubarry, Marie D'Auvergne, Rachel Ruimy, « Enjeux et réalités juridiques des Objets Connectés », *Dalloz IP/IT*, 2016, p. 394.

chiffrement des communications réalisées dans le cadre de l'Internet des objets compromet la confidentialité et l'absence d'authentification et d'identification par des mots de passe facilite indiscutablement l'accès non-protégés aux données[1071]. Trois risques principaux sont dès lors identifiés, relatifs soit à des attaques contre les objets eux-mêmes (un bracelet connecté est directement piraté), soit à des attaques réalisés grâce aux objets (le piratage du bracelet permet d'accéder aux données du téléphone auquel il est relié) ou enfin, à des attaques portant sur les communications mises en œuvre (le piratage permet de faire cesser la connexion entre le bracelet et le téléphone)[1072].

565. La nécessite d'une réponse rapide. Face au développement de ces risques et à l'essor relativement récent du domaine de l'Internet des objets, les mesures mises en œuvre par le RGPD devraient permettre une réaction plus efficace contre ce type de menaces. Le texte européen vise en effet à mettre en place un dispositif permettant une meilleure réactivité des responsables de traitement lorsque des traitements de données personnelles sont compromis. Le but de ces notifications de failles de sécurité est de pouvoir *in fine* limiter les risques qui seront causés aux individus, en donnant la capacité aux autorités administratives chargées de la protection de vérifier que les responsables de traitement proposent des solutions aux violations constatées. L'incapacité de maîtrise totale du risque est donc contrebalancée par l'apparition dans le texte européen de mesures visant à permettre une sécurisation plus efficace des dispositifs utilisés et une remontée rapide d'informations lorsque des traitements sont compromis.

La technologie utilisée tend également à offrir des garanties pour limiter les risques. Ainsi, les dispositifs employés intègrent désormais des éléments favorisant la confiance des usagers : les éléments de réglementation *ex post* maintenus sont complétés par la mise en œuvre de mesures techniques directement incorporées au sein des outils utilisés.

[1070] Jonathan Roux. *Détection d'Intrusion dans l'Internet des Objets : Problématiques de sécurité au sein des domiciles*, Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes D'Information (RESSI), Mai 2017, Grenoble, France, 2017, p. 4.

SECTION II. LA REDÉFINITION DES MODES DE RÉGULATION PAR LA TECHNOLOGIE

566. Le RGPD vise à favoriser une logique de protection en amont des données à caractère personnel traitées et la réglementation cherche à ce titre à favoriser le développement de mesures protectrices *ex ante*. Ainsi, les technologies employées doivent, en elles-mêmes, apporter des solutions à la question de la protection des données et aux risques mentionnés par le Règlement[1073]. A ce titre, le considérant 78 du texte précise directement que « la protection des droits et libertés des personnes physiques […] exige l'adoption de mesures techniques et organisationnelles appropriées » afin de respecter les exigences du Règlement. Les mesures juridiques sont aussi complétées par des mesures techniques pour assurer un traitement vertueux et *a minima* des données à caractère personnel ; le principe de minimisation des données traitées qui est instauré par le texte européen doit donc passer par la mise en œuvre d'une architecture du réseau directement protectrice des données traitées **(Paragraphe 1)**, complétée par l'intégration de standards de protection en amont de toute opération de traitement **(Paragraphe 2)**.

§1. Une architecture du réseau protectrice des données

567. La création d'une donnée à caractère personnel repose sur la traduction en langage informatique d'une information. Cette opération n'est théoriquement pas neutre car elle révèle, en amont, la mise en œuvre d'un processus guidé humainement, révélateur d'un ensemble de choix quant aux objectifs à atteindre[1074]. A l'image d'un algorithme qui ne pourra jamais être totalement empreint de neutralité[1075], la création d'une donnée sera le fruit d'une pensée humaine subjective susceptible d'influencer sa création et son traitement. Ces affirmations justifient notamment l'idée selon

---

[1071] Digital Security Econocom, *La sécurité de l'Internet des objets*, Livre Blanc, 2017, p. 23.
[1072] *Ibid*, p. 29.
[1073] Le considérant 75 mentionne, entres autres, les risques relatifs à un préjudice moral ou à un vol et à une usurpation d'identité.
[1074] Lisa Gitelman (ed.), *Raw Data is an Oxymoron*, The MIT Press, 2013, p. 4.
[1075] Gaël Chantepie, « Le droit en algorithmes ou la fin de la norme délibérée ? », *Dalloz IP/IT*, 2017, p. 522 ; Lêmy Godefroy, « Le code algorithmique au service du droit », *Recueil Dalloz*, 2018, p. 734.

laquelle le code, élément de langage informatique et de structuration du réseau, devient un élément de régulation du cyberespace. Cette théorie a notamment été développée par Lawrence Lessig pour qui « ce code, ou cette architecture, définit la manière dont nous vivons le cyberespace »[1076]. Cette proposition permet dès lors de justifier l'instauration d'une architecture du réseau directement protectrice des données qui sont traitées. L'application de l'expression « Code is law » aux données personnelles traitées, notamment dans le cadre du *quantified-self* **(A)**, s'accompagne d'un principe de neutralité technologique permettant l'efficacité de la réglementation **(B)**.

A. « Code is law »

568. L'expression « Code is Law » employé par Lessig montre que l'architecture d'un réseau informatique est susceptible d'être, en soi, porteuse de solutions propices à la mise en œuvre d'éléments de régulation technologique axés sur la protection des données à caractère personnel. Avant même l'adoption du RGPD, différents moyens permettant d'assurer leur protection, portés sur une architecture du réseau vertueuse pour les données à caractère personnel, ont été avancés. Les objets connectés utilisés dans le cadre du *quantified-self* devraient dès lors être également à même de proposer des limitations technologiques à d'éventuelles traitements non-autorisés de données. A ce titre, prévoir une obsolescence programmée des objets n'assurant plus la sécurité des données **(1)**, ainsi qu'un droit au silence des puces **(2)**, permettrait d'apporter un début de réponse aux problématiques rencontrées.

1. L'obsolescence programmée

569. La définition de la notion. Le concept d'obsolescence programmée fait l'objet de nombreux débats lorsqu'il est appliqué aux nouvelles technologies. Depuis l'adoption de la loi sur la transition énergétique du 17 août 2015, il est même constitutif d'un délit. Ce texte a permis de définir juridiquement ce concept, celui-ci

[1076] Lawrence Lessig, « Code is law, On liberty in Cyberspace », *Harvard Magazine*, January – February, 2000.

étant entendu comme « l'ensemble des techniques par lesquelles un metteur sur le marché vise à réduire délibérément la durée de vie d'un produit pour en augmenter le taux de remplacement »[1077]. Cette définition large permet de prendre en compte les différentes situations envisagées lors des débats entourant la discussion de la loi, relatives à l'obsolescence de fonctionnement, à l'obsolescence esthétique ou encore à l'obsolescence d'incompatibilité et à l'obsolescence indirecte[1078]. L'objectif annoncé de ce texte est de « protéger le consommateur contraint de remplacer un produit qu'il aurait dû, ou à tout le moins pu, conserver », celui-ci s'accompagnant de sanctions importantes à l'égard du fabricant, « à savoir deux ans d'emprisonnement et une amende d'un montant de 300 000 euros pouvant être porté à 5% du chiffre d'affaires moyen annuel »[1079]. L'obsolescence programmée a notamment été invoquée par une association contre Apple, ce dernier ayant indiqué brider la vitesse de ses dispositifs à la suite de certaines mises à jour[1080]. Une proposition de résolution du Parlement européen invite la Commission à développer un cadre européen relatif à la lutte contre l'obsolescence programmée, en promouvant notamment la réparabilité et la longévité des produits[1081], déjà évoquées au niveau national par la loi du 17 mars 2014 relative à la consommation[1082].

560. Le risque d'opposition entre lutte contre l'obsolescence et protection des données. Le débat relatif à l'obsolescence programmée pourrait être « en sérieux contraste avec d'autres aspects du mouvement général d'expansion qui se dessine »[1083]. En effet, la lutte contre l'obsolescence programmée serait paradoxalement susceptible de limiter le développement de solutions technologiques protectrices des données à caractère personnel. Allonger la durée de vie des dispositifs déjà présents sur le marché pourrait ralentir le développement d'objets mieux sécurisés et plus protecteurs des données à caractère personnel. Réminiscence du principe de précaution, l'instauration d'un délit d'obsolescence programmée serait

[1077] Article L. 441-2 du Code de la consommation.
[1078] Anne-Cécile Martin, « Le délit d'obsolescence programmée », *Recueil Dalloz*, 2015, p. 1944.
[1079] *Ibid.*
[1080] Le Monde, « Une association française porte plainte contre Apple pour « obsolescence programmée » », 27 décembre 2017, accessible en ligne : http://www.lemonde.fr/entreprises/article/2017/12/27/une-association-francaise-porte-plainte-contre-apple-pour-obsolescence-programmee_5235073_1656994.html
[1081] Parlement européen, *Rapport sur une durée de vie plus longue des produits : avantages pour les consommateurs et les entreprises*, (2016/2272(INI)), Commission du marché intérieur et de la protection des consommateurs, 9 juin 2017.
[1082] Loi n° 2014-344 du 17 mars 2014 relative à la consommation, publiée au JORF n° 0065 du 18 mars 2014.
[1083] Pierre Sirinelli, Stéphane Prévost, « Obsolescence reprogrammée », *Dalloz IP/IT*, 2018, p. 1.

ainsi susceptible de limiter les innovations porteuses de solutions protectrices de la vie privée en amont, promue par le RGPD, qu'il s'agisse du principe de minimisation ou de sécurisation du traitement.

561. L'obsolescence appliquée aux dispositifs présentant un défaut de sécurité. L'obsolescence programmée consiste, de manière générale, à faire en sorte que les dispositifs soient opérationnels le plus longtemps possible, selon certains critères de réparabilité déjà proposés[1084]. Appliquée au *quantified-self*, l'obsolescence programmée viserait au contraire à limiter la durée de vie d'un dispositif qui ne répondrait plus à certains standards technologiques permettant un traitement respectueux des données à caractère personnel. Le remplacement d'objets connectés, dont la structure présenterait avec le temps des failles de sécurité, devrait être favorisé lorsqu'il est avéré que de nouvelles solutions techniques permettant une protection renforcée des individus seraient rendu disponibles. Cette solution devrait éviter que des dispositifs deviennent désuets ou dépassés au regard de l'état des connaissances technologiques.

Complétée par un droit au silence des puces, cette amélioration doit favoriser l'intégration, par les produits proposés, de dispositifs techniques permettant en permanence la protection des données traitées.

2. Le droit au silence des puces

562. Les puces « RFID ». La particularité du *quantified-self* connecté est de permettre une automatisation des procédés de collecte et de traitement des données à caractère personnel. L'individu pouvait auparavant procéder à une automesure en entrant dans un tableau différentes constantes relevées manuellement (distance parcourue en fonction d'un temps déterminé par exemple) ou en bénéficiant de conseils prodigués par d'autres personnes (dans le cas de forums de discussion par exemple). Cependant, la connexion à Internet d'objets du quotidien et la présence de puces « RFID » intégrées au sein des dispositifs a permis non seulement un dialogue

[1084] Voir par exemple le guide de réparation des dispositifs informatiques proposé par l'ONG Greenpeace et disponible en ligne à cette adresse : https://www.rethink-it.org/en/

entre plusieurs objets mais également un recueil automatique d'informations nominatives.

Les puces « RFID », porteuses de données à caractère personnel qu'elles peuvent transmettre au gré des interactions avec d'autres objets, présentent un risque élevé au regard de la protection des données à caractère personnel. Ces risques ont été identifiés dès 2005 aux Etats-Unis par la *Federal Trade Commission* qui a notamment mis l'accent sur les capacités d'accès non autorisées par des tiers aux informations contenues dans ces puces et sur les capacités renforcées de profilage qu'elles permettent, eu égard à leur taille de plus en plus réduite[1085]. Ainsi, « la miniaturisation de ces puces les rend toujours moins détectables tout en permettant d'y stocker des données plus nombreuses, voire de les doter de senseurs et de capacité de calcul »[1086].

563. La désactivation des puces. En dehors de l'automatisation du traitement de données, les puces « RFID » posent la question de leur connexion, susceptible de mettre en œuvre un dialogue permanent avec d'autres dispositifs, sans même parfois que l'utilisateur en ait conscience. Le risque, particulièrement important avec les objets connectés utilisés dans le cadre du *quantified-self*, est qu'un individu ne puisse jamais réellement désactiver son dispositif ou que celui-ci finisse par collecter des informations nominatives à son insu, sans que celui-ci puisse maîtriser cette collecte. Une application visant à mesurer l'effort réalisé lors d'exercices physiques, proposant en complément un service de géolocalisation, pourrait ainsi continuer à localiser l'utilisateur et à transmettre ces informations au responsable de traitement sans même que la personne concernée puisse être en mesure de s'y opposer. La miniaturisation de ces technologies par le prisme du développement des nanotechnologies rend en effet certaines composantes des objets utilisés difficilement maîtrisables pour un utilisateur non-averti et constitue donc un facteur d'aggravation du risque informationnel déjà identifié. Une solution a été proposée, consistant par exemple à

[1085] Federal Trade Commission, *Radio Frequency Identification : Applications and Implications for Consumers*, A Workshop Report from the Staff of the Federal Trade Commission, March 2005, p. 13.
[1086] Yves Détraigne, Anne-Marie Escoffier, *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information*, Rapport d'information fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques, Sénat, 27 mai 2009, p. 29.

avertir l'utilisateur de la mise en fonctionnement de la puce par un signal sonore ou lumineux[1087]. La mise en œuvre d'une mesure technique complétant le dispositif juridique existant serait ainsi justifiée par le fait que ces puces peuvent collecter des informations sans aucune assistance humaine[1088], renforçant le risque d'autonomisation de ces puces et la probabilité que celles-ci échappent au contrôle de l'individu. La réunion ministérielle européenne sur les enjeux de l'Internet du futur qui s'est tenue à Nice le 6 octobre 2008 retenait déjà l'hypothèse d'une déconnexion temporaire ou permanente de ces puces[1089] et l'idée d'un véritable droit au silence des puces a été reconnue[1090].

564. Le fondement juridique de la désactivation. Les principes de la protection des données demeurent en théorie pertinents lorsqu'ils sont appliqués aux puces « RFID » contenant des données personnelles et ceux-ci justifient que les puces soient désactivées une fois leur finalité réalisée. Pourtant, au regard de la difficulté à pouvoir déterminer à partir de quand une finalité est accomplie en matière de *quantified-self*, cette proposition doit ici être écartée pour fonder le droit au silence sur d'autres principes de la réglementation, tels que le consentement préalable de l'individu, le droit à l'information ou le principe de sécurité. Le mécanisme juridique renouvelé par le RGPD doit donc théoriquement permettre de maîtriser le déploiement des puces et il a également été proposé, notamment par le G29[1091], que des évaluations d'impact sur la protection des données et sur la vie privée soient menées afin de mesurer les implications et les risques relatifs au déploiement massif de ces puces[1092].

[1087] Electronic Privacy Information Center, *Guidelines on Commercial Use of RFID Technology*, July 9, 2004, p. 2.
[1088] Kevin Ashton, « That 'Internet of Things' thing : In the real world things matter more than ideas », *RFID Journal*, June 22, 2009.
[1089] Le secrétaire d'Etat à l'économie numérique de l'époque, Eric Besson, indiquait à ce sujet que « les consommateurs devront donc pouvoir « tuer » (momentanément ou définitivement) les puces dans le cas ou celles-ci constitueraient une menace pour leur vie privée », https://www.francetvinfo.fr/sciences/high-tech/l-europe-plaide-pour-un-droit-au-silence-des-puces-rfid_1615963.html
[1090] Yves Détraigne, Anne-Marie Escoffier, *op. cit.*, p. 44.
[1091] G 29, *Avis 9/2011 sur la proposition révisée des entreprises relatives au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID)*, WP 180, 11 février 2011.
[1092] Recommandation de la Commission du 12 mai 2009 sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence [notifiée sous le numéro C (2009) 3200], (2009/387/CE), 16 mai 2009.

Selon la Commission européenne, le droit au silence des puces, pour être pleinement effectif, nécessite que les entreprises manufacturières produisent en amont des puces qui soient désactivables à tout moment et requièrent une action positive de l'individu pour être mise en fonctionnement[1093]. Mais les risques découlant du fonctionnement de ces puces peuvent également être maîtrisés par le principe de neutralité technologique affirmé par le RGPD.

B. Le principe de neutralité technologique

565. Le principe de neutralité technologique apparaissait en filigrane dans la loi Informatique et Libertés de 1978 modifiée. Il n'était pas expressément mentionné par le texte mais il pouvait être déduit du spectre élargi des termes employés. Le principe de neutralité technologique figure désormais explicitement au considérant 15 du RGPD qui indique qu'afin « d'éviter de créer un risque grave de contournement, la protection des personnes physiques devrait être neutre sur le plan technologique et ne devrait pas dépendre des techniques utilisées ». Particulièrement adapté au *quantified-self* **(1)**, le principe de neutralité technologique s'accompagne de mesures techniques visant à renforcer la protection conférée aux utilisateurs de dispositifs d'automesure **(2)**.

1. Un principe adapté au *quantified-self*

566. Le principe de neutralité technologique impose que le droit ne soit pas dépendant de la technique. Celle-ci peut éventuellement l'entraver mais elle n'est intrinsèquement « ni bonne, ni mauvaise » car elle ne porte aucune valeur, aucun choix, ni aucune directive de comportement[1094]. Le principe de neutralité implique que les règles juridiques établies ne soient pas dépendantes des techniques employées, ces dernières ne devant pas influencer l'appréciation ou la portée de ces règles. L'instauration de ce principe révèle l'impossibilité pour le droit de pouvoir anticiper avec précision les évolutions technologiques à venir. En effet, la neutralité technologique a rendu juridiquement possible le développement de l'automesure

[1093] *Ibid.*
[1094] Cyril Rojinsky, « Cyberespace et nouvelles régulations technologiques », *Recueil Dalloz*, 2001, p. 844.

connectée, sans que l'ensemble des règles juridiques instaurées nécessitent d'être entièrement rénovées. Cette neutralité technologique est pourtant susceptible de relever de l'ordre du mythe et l'architecture même du réseau présenterait intrinsèquement des éléments de régulation juridique[1095]. Mais elle doit être gage de sécurité juridique pour les personnes concernées par des traitements de données à caractère personnel.

567. Le *quantified-self* n'était à l'origine pas prévu par les différents textes juridiques en vigueur. Ceux-ci, par l'étendue des termes employés et par leur généralité, ont pourtant pu s'adapter, dans une certaine mesure, au développement de nouvelles technologies. L'imprévisibilité inhérente à l'innovation et aux nouvelles technologies nécessite donc que les règles juridiques ne soient pas rendues obsolètes par l'adoption de nouvelles techniques de collecte et de traitement de données. Ce principe est susceptible d'apporter une certaine flexibilité au régulateur qui « peut rendre son action plus efficace en permettant de s'adapter aux évolutions de l'offre ou de la demande »[1096]. Le principe de neutralité technologique trouve donc un écho particulier en matière de *quantified-self*, en raison notamment de l'impossibilité à prévoir avec certitude quels seront les objets, dispositifs ou applications qui seront utilisés à l'avenir pour la mise en œuvre de traitements de données. Dès lors, les évolutions technologiques à venir ne devraient pas impacter négativement l'application de la règlementation.

568. Le cas particulier de la *blockchain*. Le *quantified-self* n'a pas fait l'objet d'évolutions notables depuis l'entrée en application du RGPD. Mais d'autres technologies se sont développées, permettant d'illustrer l'utilité du principe de neutralité technologique. L'exemple de la *blockchain* peut être avancé, « technologie informatique permettant la création de registres décentralisés de transactions » et dont la particularité est « de se passer du recours à un tiers de confiance »[1097]. La question de la compatibilité de la *blockchain* avec les dispositions du RGPD se pose à certains

[1095] *Ibid.*
[1096] Winston J. Maxwell, Hogan Lovells, Marc Bourreau, « Les trois facettes de la neutralité technologique », *Les Cahiers de l'ARCEP*, octobre 2014, p. 17.
[1097] Yves Moreau, Chloé Dornbierer, « Enjeux de la technologie de blockchain », *Recueil Dalloz*, 2016, p. 1856.

égards[1098], mais le principe de neutralité technologique impose justement que celle-ci se développe conformément aux principes relatifs à la protection mis en œuvre par le texte européen. Surtout, plus qu'une confrontation entre ces deux éléments[1099], la technologie des chaînes de blocs serait susceptible de faciliter l'application de certains principes du Règlement général européen, tels que le principe de sécurité [1100], et de permettre un meilleur contrôle aux individus sur leurs données à caractère personnel[1101]. En effet, la *blockchain* pourrait permettre, en ajoutant une chaîne à l'objet connecté, de limiter le nombre de communications à d'autres supports. Dès 2015, la division santé de la société Philips a fait appel à Tierion, une entreprise spécialisée dans la *blockchain*, afin de développer des solutions sécurisées pour ses dispositifs connectés[1102].

L'utilité du principe de neutralité technologique se révèle ainsi double. D'abord, ce principe doit garantir la pertinence de la réglementation lorsqu'elle est confrontée à l'apparition de nouvelles technologies. Mais la neutralité technologique doit également permettre à de nouvelles technologies de contribuer à l'efficacité des règles protectrices. A ce titre, le RGPD prône, pour la mise en œuvre d'une protection en amont des données traitées, le développement du recours à la cryptologie afin d'assurer une meilleure protection des données recueillies.

2. Un principe complété par la cryptologie et l'anonymisation

569. Le recours au chiffrement. La CNIL était, sous l'empire de la loi Informatique et Libertés de 1978, chargée de promouvoir l'utilisation des technologies protectrices de la vie privée, parmi lesquelles les technologies de chiffrement des données[1103]. Vague dans son étendue et sa mise en œuvre pratique, ce recours au chiffrement est désormais généralisé et précisé par le RGPD qui indique

[1098] AFCDP, « La blockchain est-elle soluble dans le RGPD ? », Compte-rendu de l'intervention de Bruno Rasle, délégué général de l'AFCDP, lors de l'assemblée générale de l'AFCDP qui s'est tenue à Paris le 21 juin 2017, disponible en ligne à cette adresse : https://www.afcdp.net/La-Blockchain-est-elle-soluble
[1099] Nathalie Devillier, « Jouer dans le « bac à sable » réglementaire pour réguler l'innovation disruptive : le cas de la technologie de la chaîne de blocs », *RTD com*, 2017, p. 1037.
[1100] Primavera De Filippi, Aaron Wright, *Blockchain & Droit, le règne du code*, Dicoland, mai 2019, 296 p.
[1101] Florence Chafiol, Alice Barbet-Massin, « La blockchain à l'heure de l'entrée en application du règlement général sur la protection des données », *Dalloz IP/IT*, 2017, p. 637.
[1102] https://bitcoinist.com/tierion-philips-bring-blockchain-technology-healthcare-sector/
[1103] Loi 78-17 du 6 janvier 1978, article 11, 4°, f)

que le chiffrement peut être utilisé pour limiter les risques qui sont inhérents au traitement mais également pour assurer la sécurité de celui-ci[1104]. Apprécié au regard de plusieurs critères relatifs aux coûts de mise en œuvre, au contexte et aux finalités du traitement, la nécessité de mettre en place des solutions de chiffrement des données repose sur l'appréciation du risque susceptible d'être engendré, au regard de sa probabilité et de sa gravité[1105]. Historiquement et étymologiquement, la cryptologie correspond à la science du secret et le chiffrement « permet justement de garantir que seuls l'émetteur et le(s) destinataire(s) légitime(s) d'un message en connaissent le contenu » et donc de le rendre inaccessible et illisible, faute d'avoir la clé spécifique[1106].

L'utilisation du chiffrement appliqué aux données à caractère personnel permettrait donc de rendre les données uniquement lisibles pour les responsables de traitement (et sous-traitants éventuels) et pour les personnes concernées par le traitement, destinataires de la clé de sécurité. Le RGPD impose la mise en œuvre de mesures techniques pour garantir la sécurité des informations collectées et des traitements mis en œuvre, mais le recours au chiffrement n'est pourtant pas rendu obligatoire. Le caractère impératif de cette mesure a pourtant fait l'objet de discussions au niveau national. L'adoption de la loi relative à la protection des données personnelles qui a adapté le droit français au RGPD a ainsi opposé l'Assemblée Nationale et le Sénat sur la question du chiffrement. Les sénateurs avaient adopté, contre l'avis du gouvernement, un amendement qui visait à rendre le chiffrement obligatoire pour les sites traitants des données à caractère personnel. La question de la mise en œuvre obligatoire de ces mesures techniques a donc été posée[1107], même si le texte définitivement adopté le 14 mai 2018 n'a pas retenu cette solution. En effet, même si le chiffrement semble être une réponse possible au risque informationnel, celui-ci est limité en pratique par la complexité relative à sa mise en œuvre : appliqué au *quantified-self*, celui-ci impliquerait que toutes les

[1104] L'article 32 du texte indique que « le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins : la pseudonymisation et le chiffrement des données à caractère personnel ».
[1105] Règlement (UE) 2016/679, considérant 32.
[1106] CNIL, « Comprendre les grands principes de la cryptologie et du chiffrement », 25 octobre 2006, disponible en ligne à cette adresse : https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement
[1107] Assemblée Nationale, Projet de loi relatif à la protection des données personnelles, texte adopté n° 113, 14 mai 2018.

communications soient chiffrées, ce qui constituerait une lourde charge pour les responsables de traitement.

D'autres mesures techniques, telles que la pseudonymisation et l'anonymisation, permettent également d'éviter ou de limiter les éventuelles atteintes aux traitements mis en œuvre.

570. L'anonymisation et la pseudonymisation. La question de l'anonymisation est directement mentionnée par le RGPD qui indique, au considérant 26, qu'il n'y a « pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable ». Le fait que la personne concernée ne soit pas ou plus identifiable, en raison de l'anonymisation de ses informations, fait sortir les données en question du cadre de la réglementation. L'anonymisation, qui empêche de manière irréversible l'identification, ne constitue dès lors pas une mesure technique de protection des données à caractère personnel : elle a pour but de dépersonnaliser de telles informations. Un processus d'anonymisation constitue en soi un traitement de données à caractère personnel, puisque celles-ci sont à l'origine du procédé et le G29 a dégagé trois critères permettant d'en apprécier la pertinence. Trois éléments doivent ainsi être étudiés, relatifs d'abord à l'individualisation (est-il toujours possible d'isoler un individu ?), à la corrélation (est-il possible de relier entre eux des ensembles de données distincts concernant un même individu ?) et enfin à l'inférence (peut-on déduire de l'information sur un individu ?)[1108]. La CNIL et le Conseil d'Etat veillent à la solidité des processus d'anonymisation mis en œuvre, comme en témoigne un arrêt rendu le 8 février 2017. En l'espèce, une société avait déposé une demande d'autorisation à la CNIL afin de pouvoir installer des boîtiers de comptage sur du mobilier urbain. Ceux-ci devaient permettre de collecter les identifiants (adresse MAC pour *Media Access Control*) d'appareils mobiles afin de mesurer le taux de fréquentation. La société devait ensuite procéder à l'anonymisation des informations collectées. Pourtant, pour la CNIL[1109], les mesures mises en œuvre ne

[1108] G29, Avis 05/2014 sur les Techniques d'anonymisation, WP 216, adopté le 10 avril 2014, p. 13.
[1109] Délibération n° 2015-255 du 16 juillet 2015 refusant la mise en œuvre par la société JCDecaux d'un traitement automatisé de données à caractère personnel ayant pour finalité de tester une méthodologie d'estimation quantitative des flux piétons sur la dalle de La Défense (demande d'autorisation n° 1833589).

permettaient pas de procéder à l'anonymisation car la société était encore en mesure de rejouer le procédé de chiffrement. Le Conseil d'Etat, confirmant la décision de la CNIL, a également indiqué que le procédé employé ne constituait pas une mesure d'anonymisation car il laissait « le gestionnaire du traitement en mesure de procéder à l'identification des personnes concernées »[1110].

571. L'arrêt du Conseil d'Etat soulève la distinction entre anonymisation et pseudonymisation, qui « consiste à remplacer un attribut par un autre dans un enregistrement » et qui implique donc, sans recours à des informations supplémentaires, que la personne soit « toujours susceptible d'être identifiée indirectement »[1111]. En effet, la pseudonymisation peut impliquer le recours au chiffrement, mais elle ne permet pas une complète anonymisation des données traitées[1112]. Par exemple, le responsable de traitement d'une application de *quantified-self* pourrait procéder à la pseudonymisation des données identifiantes récoltées en les remplaçant par d'autres informations (un nom remplacé par un symbole). Mais dans ce cas, le responsable de traitement aurait toujours la possibilité d'identifier la personne ; c'est en effet lui qui a décidé du symbole permettant de remplacer l'information identifiante.

Le RGPD mentionne pourtant explicitement la pseudonymisation comme élément technique et organisationnel permettant une protection renforcée des données à caractère personnel et une sécurité renforcée du traitement. En effet, celle-ci peut tout de même « réduire les risques pour les personnes concernées et aider les responsables du traitement et les sous-traitants à remplir leurs obligations en matière de protection des données »[1113]. La pseudonymisation participe dès lors à la réalisation de la conformité permanente exigée par le nouveau cadre européen et pesant sur les responsables de traitement. Cette mesure permet également le respect du principe de minimisation des données qui implique que seules les données nécessaires à la réalisation de la finalité déterminée soient collectées.

[1110] CE, 8 février 2017, n° 393714, Mentionné dans les tables du recueil Lebon.
[1111] G29, *op. cit.*, p. 22.
[1112] Le considérant 26 du Règlement précise que « les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable ».
[1113] Considérant 28, Règlement (UE) 2016/679.

572. Les limites de ces procédés. L'anonymisation et la pseudonymisation peuvent dans certains cas constituer une réponse efficace au risque informationnel pesant sur l'individu. Pourtant, les limites techniques de ces différents procédés constituent un frein à leur déploiement automatique. La pseudonymisation ne vient pas changer la nature des données traitées : celles-ci demeurent identifiantes et une réidentification par le responsable de traitement ou une tierce partie reste possible[1114]. Il en va de même concernant l'anonymisation, celle-ci ne permettant pas une sécurité infaillible des données collectées lorsque des traitements sont mis en œuvre[1115]. En effet, malgré l'évolution des procédés techniques permettant de procéder à l'anonymisation, la masse d'informations désormais disponible publiquement pour chaque individu fait que les possibilités de corrélation et d'identification sont facilitées.

Par exemple, l'application de *fitness* Strava, qui permet de centraliser les données sportives d'utilisateurs, avait mis en ligne une cartographie des données d'activité agrégées, montrant les parcours favoris des individus sans pouvoir directement les identifier. Cette cartographie permettait d'abord d'inférer des zones sensibles : il était en effet possible, en suivant l'activité de militaires portant des *trackers* d'activité, de distinguer les contours précis de leurs bases et de les localiser lorsque ceux-ci couraient autour pour s'entraîner[1116]. Ensuite, un chercheur en sécurité informatique a révélé que la cartographie réalisée rendait possible l'obtention des noms et parcours d'utilisateurs dans une même zone géographique[1117] . Enfin, un autre élément permettait d'identifier l'individu. Lors de marathons, le nom ainsi que le temps réalisé sont généralement disponibles sur le site Internet de l'organisateur. Dans ce cas, peu importe que les données d'un *tracker* d'activité soient anonymisées : il suffit, pour identifier la personne, de comparer la donnée relative au temps (par exemple, le fait que l'individu ait couru le marathon en 04h15 minutes) avec la liste

[1114] Florence Raynal, « De nouvelles dispositions pour protéger les données personnelles », *Documentaliste-Sciences de l'Information*, vol. 51, n°3, 2014.
[1115] Arvind Narayanan, Edward W. Felten, « No silver bullet : De-identification still doesn't work », *White Paper*, 2014, p. 2
[1116] Olivier Desbiey, « Strava : la Heat Map qui fait froid dans le dos », *Laboratoire d'Innovation Numérique de la CNIL (LINC)*, 29 janvier 2018, en ligne : https://linc.cnil.fr/fr/strava-la-heat-map-qui-fait-froid-dans-le-dos
[1117] Steve Loughran, Advanced Deanonymization through Strava, 29 janvier 2018, en ligne : http://steveloughran.blogspot.com/2018/01/advanced-denanonymization-through-strava.html

de l'organisateur (en recherchant l'individu ayant parcouru le marathon en 04h15 minutes).

Le RGPD, au regard de ces différentes limites relatives à la pseudonymisation et à l'anonymisation, va surtout dans le sens de l'intégration de différents standards de protection en amont. La portée de certains de ces standards est en pratique limitée, mais ceux-ci doivent permettre, par leur diversité, une meilleure protection des données traitées.

§2. L'intégration de standards de protection en amont

573. Les objets connectés ont pour particularité de changer le mode de production des données à caractère personnel. Celui-ci, devenu automatique et permanent, contribue à une collecte exponentielle d'informations nominatives. Le volume d'informations traitées dans ce cadre complexifie dès lors l'applicabilité de la règlementation, celle-ci étant fragilisée par la présence d'un important nombre de traitements mis en œuvre de façon automatique. Le RGPD, prenant en compte ces développements technologiques, vise à favoriser la protection en amont des données à caractère personnel, avant même la mise en œuvre des procédés de collecte. Cette protection en amont vise à limiter le nombre d'informations traitées grâce au principe de minimisation de la collecte. La problématique relative à la vie privée est dès lors directement intégrée aux procédés de recueil des données. Ainsi, les technologies employées, selon l'idée que le code fait loi, permettent de garantir techniquement le respect des informations traitées. Un concept de vie privée dès la conception des traitements est né **(A)**, complété par une utilisation raisonnée des dispositifs par les individus, dont les pratiques permettront ainsi de limiter directement le risque informationnel **(B)**.

A. La « Privacy by design »

574. La *Privacy by design*, ou protection de la vie privée et des données personnelles dès la conception, suppose la mise en œuvre de mesures techniques et organisationnelles dès le développement de systèmes de traitements de données à

caractère personnel. Ce principe de protection dès la conception, outil permettant d'assurer la conformité à la réglementation[1118], est explicitement instauré par le RGPD qui y consacre un article 25. Complété par un principe de protection des données par défaut, celui-ci doit permettre « de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée ». Il impose ainsi « au concepteur de la technologie de prendre en compte les risques d'atteinte aux données personnelles en amont du projet et de prévoir toutes les mesures nécessaires pour les protéger »[1119]. Le concept de protection en amont et par défaut n'est pas nouveau et la doctrine a déjà pu le développer[1120]. Mais sa consécration au sein du RGPD a semblé nécessaire au regard des développements techniques permis par les objets connectés utilisés pour la pratique du *quantified-self* **(1)**. Pourtant, sa mise en œuvre concrète présente encore certaines difficultés **(2)**.

1. Une évolution nécessaire

575. Le RGPD procède à un renversement des mécanismes de protection précédemment instaurés. De l'incapacité à maîtriser avec certitude l'ensemble exponentiel de données traitées et collectées à différentes échelles est née une logique de responsabilisation des responsables de traitements. Le principe de protection dès la conception doit participer de ce changement de paradigme en accentuant la mise en œuvre d'une protection *ex ante* des informations récoltées. L'immatérialité, propre à chaque donnée créée et collectée, fait que celles-ci ne se dégradent pas par l'usage qui peut en être fait. Surtout, celles-ci deviennent difficilement traçables après leur création, ce qui rend toute possibilité de maîtrise *a posteriori* difficile voire illusoire, au regard notamment du volume de données créées par les objets connectés dans le cadre du *quantified-self*. Les principes de protection dès la conception et de protection par défaut permettent dès lors de répondre à ces problématiques, respectivement avant et après la création d'une donnée à caractère personnel ou d'un traitement.

[1118] Le considérant 78 du Règlement (UE) 2016/679 précise ainsi qu'afin « d'être en mesure de démontrer qu'il respect le présent règlement, le responsable du traitement devrait adopter des règles internes et mettre en œuvre des mesures qui respectent, en particulier, les principes de protection des données dès la conception et de protection des données par défaut ».
[1119] Gérard Haas, *Le RGPD expliqué à mon boss*, Editions Kawa, décembre 2017, p. 123.

576. Initialement développé au Canada à la fin des années 90 par Ann Cavoukian, commissaire à la protection des données de l'Ontario, le concept de *Privacy by design* repose sur l'intégration de sept principes distincts[1121] : approche proactive de la protection des données, protection par défaut, intégration de dispositifs protecteurs au sein de l'objet, somme positive d'avantages pour l'individu et le responsable du traitement, sécurité tout au long de la chaîne du traitement, transparence et respect du rôle central de l'usager sont autant d'éléments qui fondent le principe de *Privacy by design*. Ces différents éléments s'inscrivent dans le prolongement du principe d'autodétermination informationnelle dégagé par la Cour constitutionnelle fédérale d'Allemagne en 1983. La personne concernée par le traitement doit en permanence être placée au cœur du dispositif protecteur et celle-ci doit avoir la maîtrise des informations qui sont collectées et traitées. Cette maîtrise devra être rendue possible tout au long de la chaîne de traitement de la donnée et suppose donc que les procédés de *Privacy by design* soit affinés et précisés au fil du temps.

577. Le concept de *Privacy by design*, rapidement identifié par les autorités européennes comme une solution permettant de garantir la protection des données issues d'objets connectés[1122], « entend pallier les limites que rencontrent les réglementations pour protéger les données à caractère personnel dans le cadre de ces nouveaux usages »[1123]. Relais technique du cadre réglementaire, « cette méthodologie permet encore de dépasser les limites que rencontrent les autorités de régulation dans leur pouvoir d'intervention »[1124]. Plus qu'un simple principe de précaution appliqué directement au processus de collecte et de traitement des données à caractère personnel, la protection dès la conception suppose que la technologie soit directement mise au service de la protection des données. Sans désigner de techniques précises,

---

[1120] Ann Cavoukian, « Privacy by design [leading edge] », *IEEE Technology and Society Magazine*, vol. 31, n°4, 2012, p. 18 à 19.
[1121] Ann Cavoukian, « Privacy by Design, The 7 Foundational Principles », *Information and Privacy Commissioner of Ontario*, January 2011.
[1122] Voir par exemple : Communication de la Commission du 18 juin 2009, COM (2009) 278 final, « L'Internet des objets, un plan d'action pour l'Europe », p. 7.
[1123] Célia Zolynski, « La Privacy by Design appliquée aux Objets Connectés : vers une régulation efficiente du risque informationnel ? », *Dalloz IP/IT*, 2016, p. 404.
[1124] *Ibid.*

cette protection s'entend d'une méthodologie à déployer par le responsable de traitement pour parvenir à la conformité du traitement réalisé. L'incorporation de procédés de pseudonymisation déjà évoqués au sein des objets utilisés peut à ce titre entrer dans le cadre de la *Privacy by design*, bien qu'ils ne soient pas exclusifs de la mise en œuvre d'autres mécanismes techniques ou organisationnels protecteurs, montrant la liberté des responsables de traitements quant aux solutions à apporter. Un principe de proportionnalité est par ailleurs instauré par le RGPD, la mise en œuvre de mécanismes de protection dès la conception étant subordonnée à l'appréciation du risque pour les droits et libertés des personnes physiques engendré par le traitement, au regard du coût de ces différentes mesures, de la portée, du contexte et des finalités du traitement.

578. La protection par défaut. Le principe de protection dès la conception est complété par un principe de protection par défaut des données traitées. Reposant également sur la mise en œuvre de mesures techniques et organisationnelles appropriées, ce principe fait référence à une collecte *a minima* des données traitées, puisque seules celles qui sont nécessaires « au regard de chaque finalité spécifique du traitement » sont traitées[1125]. Ce principe de protection par défaut implique dès lors que la confidentialité des informations soit assurée et que les données ne soient pas rendues disponibles « à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée »[1126]. En matière d'objets connectés ou d'applications de *quantified-self*, cela devra notamment signifier que lorsqu'un individu commence à utiliser un tel dispositif, les paramètres du dispositif en question devront, par défaut, assurer une confidentialité renforcée des données collectées. Les applications de *running* permettant de procéder à la géolocalisation des individus devraient donc garantir, par défaut et avant la collecte, que les informations relatives aux trajets d'un individu ne seront pas transmises à des tiers ou rendues publiques.

Les principes de protection dès la conception et de protection par défaut constituent ainsi une avancée certaine en matière de régulation mais les difficultés

[1125] Article 25 du Règlement (UE) 2016/679.
[1126] *Ibid.*

pratiques de mise en œuvre auxquelles ils sont confrontés sont susceptibles d'en limiter la portée.

2. Les difficultés de mise en œuvre

579. La généralité du principe. La mise en œuvre concrète des principes de *Privacy by design* confirme l'orientation nouvelle prise par la réglementation, fondée sur une logique de conformité. Forme de régulation *ex ante*, celle-ci vise à prévenir le risque informationnel pesant sur les personnes concernées par des traitements de données, que celui-ci se réalise ou non. Mesure préventive, la protection dès la conception relève d'un concept large qui « peut s'appliquer aussi bien à des terminaux qu'à des systèmes d'information »[1127]. Celle-ci peut dès lors être directement intégrée aux objets connectés utilisés dans le cadre du *quantified-self*, mais également aux procédés de traitement de données qui sont mis en œuvre par la suite, tels que l'analyse et l'étude statistique des données collectées. Ces différents éléments devront donc directement proposer des solutions fondées sur les principes fondateurs de la *Privacy by design*. Pourtant, « nombreux sont ceux qui s'accordent sur le flou qui entoure les termes très généraux de ces principes »[1128] et la traduction concrète en mesures à adopter pour les responsables de traitements semble difficile à apprécier. La pseudonymisation est explicitement mentionnée parmi les mesures susceptibles d'être adoptée mais la question des autres mesures techniques ou organisationnelles concrètes à déployer reste en suspens, en l'attente d'un éventuel pack de conformité proposé par la CNIL[1129].

580. L'application limitée par la finalité du *quantified-self*. L'implémentation du principe de *Privacy by design* doit permettre une meilleure protection en amont des données traitées, mais ce principe s'oppose dans certains cas aux modalités de fonctionnement même des objets connectés et du *quantified-self*.

[1127] Alain Rallet, Fabrice Rochelandet, Célia Zolynski, « De la Privacy by Design à la Privacy by Using. Regards croisés droit/économie », *Réseaux*, 2015/1, n° 189, p. 15-46.
[1128] Matthieu Dary, Leila Benaissa, « Privacy by Design : un principe de protection séduisant mais complexe à mettre en œuvre », *Dalloz IP/IT*, 2016, p. 476.
[1129] Voir par exemple : CNIL, *Pack de conformité Véhicules connectés et données personnelles*, octobre 2017, p. 16, dans lequel elle fait directement référence à la question de la protection des données dès la conception sans pour autant en développer les mesures susceptibles d'être mises en œuvre.

Ceux-ci, reposant sur une collecte exponentielle de données, s'inscrivent dans une logique d'économie « behavioriste » selon laquelle la qualité et l'intérêt du service proposé dépendent du volume d'informations révélées par les individus. Dans le cadre de l'automesure connectée, plus la divulgation d'éléments relatifs à l'intimité, au corps et à l'activité physique est importante, plus la précision du retour formulé à l'utilisateur par le responsable du traitement sera améliorée. Dès lors, instaurer une protection *ex ante* visant à limiter le nombre d'informations traitées et à incorporer des mesures techniques directement au sein des objets utilisés serait susceptible de nuire au fonctionnement de ces outils et d'en limiter les possibilités d'utilisation. L'instauration d'un principe de protection en amont serait ainsi contraire au fait que la divulgation de données à caractère personnel est une condition d'existence du service lui-même.

581. Les enjeux économiques. La *Privacy by design* s'inscrit dans une logique de conformité visant à éviter la lourdeur d'une déclaration administrative préalable à l'autorité de contrôle en charge de la protection des données. Mais elle est susceptible d'entraîner de nombreuses difficultés pratiques pour les responsables de traitements. Devant assurer la mise en œuvre du principe de protection dès la conception et de protection par défaut à l'ensemble de la chaîne de traitements, le risque est que le nombre de services proposés soit limité en raison de l'ampleur des moyens à mettre en œuvre. Les grandes entreprises ne devraient pas être affectées par ces mesures. Les moyens financiers dont elles disposent et qui sont notamment alloués à la recherche et au développement devraient leur permettre de développer de nouvelles solutions protectrices des données à caractère personnel. Mais de telles procédés sont surtout susceptibles d'impacter les entreprises de taille moyenne ou réduite. Les innovations technologiques qu'elles proposent pourraient être limitées en raison du coût et de la diversité des mesures à adopter et dont la fiabilité a été pour certaines remise en question par le Sénat[1130].

Le RGPD, actant cette disparité entre entreprises, favorise le développement et l'élaboration de codes de conduite tenant compte, en vertu de l'article 40, de « la

[1130] Voir notamment : Gaëtan Gorce, François Pillet, *op. cit.*, p. 43 et s. à propos des risques de ré-identification permis par l'anonymisation, la pseudonymisation, l'ajout de bruit ou l'agrégation.

spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises ». Ces codes de conduite peuvent ainsi porter sur les mesures visées à l'article 25, relatives à la protection dès la conception et à la protection par défaut des données. Un projet de code de conduite relatif aux applications de santé mobile a ainsi été publié[1131], bien que non accepté par le groupe de l'article 29[1132]. Applicable spécifiquement aux données de santé, ce document préconise une désactivation par défaut des modalités de partage de données permises par les applications.

582. Ainsi, limiter en amont le nombre d'informations collectées par un objet connecté, utilisé par exemple en santé, constituerait une limite à la découverte d'éléments nouveaux. Procédure de filtrage visant à responsabiliser les opérateurs du numérique au regard des moyens d'actions limités des autorités de contrôle, l'instauration d'une *Privacy by design* à l'égard des objets connectés pourrait ainsi s'inscrire en contradiction du principe de somme positive identifié par Ann Cavoukian et selon lequel le service ne doit pas être affecté ou dégradé par la mise en œuvre concrète de mesures *ex ante*. La question se pose ainsi de savoir si l'instauration de mesures protectrices en amont ne serait pas susceptible de limiter les potentialités offertes par le *quantified-self*.

A ce titre, une solution complémentaire à celle de protection dès la conception a été proposée, impliquant l'apprentissage et la mise en œuvre de normes sociales de *privacy* directement par l'individu.

B. La « Privacy by using »

583. Face à la complexité de mise en œuvre concrète de mesures de *Privacy by design* et de protection par défaut, plusieurs auteurs ont proposé une solution complémentaire à la protection des données dès la conception. Solution qui procèderait à un second changement de paradigme de la régulation, des entreprises aux individus, celle-ci permettrait une responsabilisation des personnes concernées

[1131] European Commission, *Draft Code of Conduct on privacy for mobile health applications*, June 7th, 2016.
[1132] Lettre adressée par le groupe de l'article 29 le 10 avril 2017 à l'éditeur du projet de code de conduite relatif aux applications de santé mobile.

par des traitements de données, en opposition au *privacy paradox*. La *Privacy by using* reposerait sur une meilleure compréhension, par les individus, des problématiques relatives à la protection des données à caractère personnel, leur garantissant ainsi une véritable autodétermination informationnelle. Celle-ci leur permettrait, à l'image de l'obligation de conformité pesant sur les responsables de traitement, d'avoir un rôle actif quant aux modalités de protection des données à caractère personnel instaurées. Corollaire de l'obligation d'information renforcée pesant sur les responsables de traitement en vertu du Règlement européen, ce principe confirme le rôle central de l'usager quant à la protection de ses données à caractère personnel **(1)** et ce grâce à l'apprentissage des normes sociales de *privacy* et à une utilisation raisonnée des dispositifs connectés **(2)**.

1. Le rôle central de l'usager

584. La *Privacy by design*, née de l'idée que la règlementation juridique est incapable d'assurer une protection efficace des données à caractère personnel, nécessite de « procéder à une veille constante des techniques et des risques nouveaux » ou encore « d'effectuer des analyses périodiques de risque » qui implique notamment des lourdeurs sur le plan organisationnel[1133]. L'implémentation de mesures de *Privacy by using* permettrait dès lors de réduire le besoin de recourir à ces différentes mesures organisationnelles en conférant un rôle actif à l'individu dans la mise en œuvre de traitements respectueux des données à caractère personnel. Cette protection des données à caractère personnel par l'usage qui est fait des dispositifs déporte ainsi le filtre de protection des exploitants vers les individus et conduit à ce que ceux-ci « soient le sujet actif de la gestion de leurs données »[1134]. Cette solution s'oppose ainsi aux principes développés dans le cadre de la *Privacy by design*. Dès lors, seul le rôle central conféré à l'usager dans le déploiement de solutions protectrices de données à caractère personnel serait susceptible d'instaurer une réelle protection *ex ante*.

[1133] Célia Zolynski, Philippe Pucheral, Alain Rallet, Fabrice Rochelandet, « La Privacy by design : une fausse bonne solution aux problèmes de protection des données personnelles ? », *Légipresse*, n° 340, Juillet-Août, 2016, p. 30.
[1134] *Ibid*., p. 36.

La *Privacy by using* regroupe les instruments technologiques, juridiques ou informationnels permettant de développer la maîtrise des normes de *privacy* par les individus. Plus qu'un outil technique, elle englobe un ensemble diversifié de procédés qui permettront *in fine* aux personnes concernées par des traitements de savoir comment limiter directement l'impact de l'utilisation de dispositifs numériques.

585. Si cette maîtrise peut être favorisée par les responsables de traitement lorsqu'ils mettent à disposition des outils techniques permettant aux individus de limiter la quantité d'informations et de traces dévoilées[1135] , le choix du recours à ce type d'outils dépendra du niveau de connaissances de l'individu, soulignant l'importance de l'apprentissage des normes sociales relatives à la *privacy* et à la protection des données à caractère personnel.

2. L'apprentissage des normes sociales de *privacy*

586. Le rôle central de l'utilisateur. La *Privacy by using* repose, pour sa mise en œuvre, sur le constat que la vie privée et la protection des données à caractère personnel sont des constructions sociales et évolutives dont les composantes varient au gré des époques et des évolutions technologiques. La notion de *privacy*, initialement dégagée par les auteurs Samuel D. Warren et Louis D. Brandeis à la fin du XIXème[1136] siècle, serait dès lors susceptible d'acceptions diverses. Le sens de cette notion pourrait également varier en fonction des expériences et des pratiques[1137]. Concernant au départ la photographie et la structuration du marché de la presse, la notion de *privacy* a ensuite été utilisée pour la protection des données à caractère personnel. L'évolution de la notion de *privacy* permettrait de justifier aujourd'hui la période de *privacy paradox* dans laquelle nous nous situons. Les individus, parce qu'ils ont aujourd'hui accès à un nombre important de services gratuits grâce à leurs *smartphones* et objets connectés, seraient moins soucieux de la protection de leur vie privée et de leurs données. Ce phénomène, rendu possible par le développement de

[1135] Voir à ce titre le cas des extensions pour navigateur web qui permettent de limiter le nombre de données traitées ou de bloquer certaines fonctionnalités indésirables. L'extension Privacy Badger permet par exemple de bloquer les sites tiers qui suivent les habitudes de navigation des individus ou les cookies qui ne respectent pas le réglage du navigateur alors que l'extension Adblock permet de limiter le nombre de publicités en ligne.
[1136] Samuel D. Warren, Louis D. Brandeis, « The Right to Privacy », *Harvard Law Review*, vol. 4, n°5, Dec. 15, 1890 pp. 193-220.

technologies toujours plus poussées, conduirait ainsi les individus à révéler des informations toujours plus intimes. De nombreux modèles économiques, dont celui du *quantified-self*, reposent sur cette logique.

L'objectif de la *privacy by using* serait dès lors d'établir un équilibre et de faire des individus des utilisateurs éclairés des services numériques, au fait des enjeux relatifs à la protection des données. Pour les auteurs appelant à l'instauration d'un modèle de protection reposant sur la *privacy by using*, celle-ci serait en effet un « processus de régulation par accumulation d'apprentissages », permettant de mettre l'individu « en capacité de mieux définir son comportement de protection de sa vie privée »[1138]. La *privacy by using* place donc l'individu au centre du dispositif protecteur des données à caractère personnel. Celui-ci, par ses choix, deviendrait le principal acteur de la protection qui lui est conférée. Il pourrait dès lors choisir d'utiliser un moteur de recherche plus respectueux de ses données ou utiliser une application payante qui ne transmet pas de données personnels à des régies publicitaires.

587. Les limites du dispositif. La *privacy by using* semble aujourd'hui progresser. Elle se nourrit en effet, depuis 2013 et les révélations d'Edward Snowden, d'une actualité fournie en matière de protection des données. Par ailleurs, elle est rendue possible par le développement de services qui visent à promouvoir la protection des données. Le moteur de recherche français Qwant, lancé en 2013, indique par exemple ne pas tracer ses utilisateurs ou ne pas revendre de données à des fins publicitaires. Des extensions créées pour d'autres moteurs de recherche permettent également de limiter les hypothèses de suivi en ligne. Pourtant, ces fonctionnalités restent encore peu nombreuses à l'heure actuelle et la *privacy by using* présente, en elle-même, des limites qui ne permettent pas d'assurer une protection infaillible des données traitées. En effet, adopter un comportement éclairé implique certaines contraintes pour les individus, qu'il s'agisse du temps consacré à la lecture attentionnée de l'ensemble des conditions générales d'utilisation de différents

[1137] Phillip Nelson, « Information and Consumer Behavior », *Journal of Political Economy*, vol. 78, n° 2, 1970, pp. 311-329.
[1138] Célia Zolynski, Philippe Pucheral, Alain Rallet, Fabrice Rochelandet, art. précité, p. 30.

services, du paiement d'un prix pour avoir accès à une application respectueuse des données ou du manque de fonctionnalités de certains services. Le niveau d'avantages donnés peut dès lors sembler résiduel au regard de l'ensemble des contraintes à surmonter. Dans le cadre du *quantified-self*, de nombreuses applications développées avant l'entrée en application du RGPD sont aujourd'hui plébiscitées par les utilisateurs, malgré des politiques de confidentialité manquant parfois de clarté[1139]. Ces applications, destinées à la mesure du bien-être, ont également tendance à fidéliser les utilisateurs par la permanence des mesures réalisées. Un sportif visant à améliorer ses performances sur le long terme et utilisant la même application depuis plusieurs années sera peu enclin à changer et préférera recevoir de la publicité plutôt que de se tourner vers un autre service, même si ce dernier est plus respectueux de ses données.

588. Un complément nécessaire. Les éléments de *privacy by using* peuvent aujourd'hui compléter les mesures de conformité auxquelles les responsables de traitement sont soumis. Ainsi, outre le contrôle réalisé par les autorités de protection, les individus, par leurs choix, participent également à ce contrôle en écartant les services qui ne traitent pas leurs données conformément à la réglementation. Ces choix devraient ainsi permettre « de faire émerger une norme sociale de la vie privée qui soit en phase avec la dynamique de développement de l'économie numérique »[1140]. L'instauration de cette norme sociale de la vie privée nécessitera cependant, avant d'être efficace, l'écoulement d'un certain temps. En effet, l'émergence des problématiques relatives à la protection des données reste encore relativement récente. L'adoption du RGPD permet cependant, par le changement de paradigme mis en œuvre, de faciliter la mise en place de ces normes sociales de *privacy* en mettant à contribution tous les acteurs concernés.

589. Conclusion du chapitre. Le RGPD procède à un déplacement des mécanismes protecteurs des données. Longtemps et presque exclusivement le fait d'autorités administratives indépendantes, ces mécanismes relèvent désormais également des responsables de traitements, devenus des acteurs à part entière de la

[1139] Cf, *supra*, n° 291.
[1140] Célia Zolynski, Philippe Pucheral, Alain Rallet, Fabrice Rochelandet, art. précité, p. 30.

protection des données à caractère personnel. Différents instruments ont été prévus par le texte pour permettre aux entreprises d'attester de leur conformité à la réglementation et pour limiter les risques pouvant résulter de traitements de données. Règles d'entreprise contraignantes, analyses d'impact sur la protection des données, *privacy by design* ou encore notification de failles de sécurité sont autant d'éléments consacrés par le texte afin de garantir la transparence des opérations réalisées par les responsables de traitement. Ce changement de paradigme permet un meilleur encadrement des opérations réalisées dans le cadre de l'automesure. Les tensions auxquelles le *quantified-self* soumet certaines définitions (donnée sensible, donnée de santé, métadonnée) et certains principes de protection (finalité déterminée, proportionnalité, durée de conservation limitée) n'ont pas totalement disparu. Mais la particularité du RGPD est d'avoir implicitement intégré ces limites pour que de telles tensions n'empêchent pas l'autodétermination informationnelle. L'identification des risques, en amont des traitements, permet ainsi la création d'un droit protecteur sur mesure, en fonction des enjeux de chaque opération.

CHAPITRE II – LE RENOUVELLEMENT DE LA RÉGULATION PUBLIQUE

590. Le RGPD opère un changement de paradigme quant à la protection apportée aux traitements de données à caractère personnel. L'Etat et la CNIL étaient auparavant au cœur du dispositif protecteur mais ce dernier repose désormais essentiellement sur les responsables de traitements ; entreprises et personnes publiques en charge de collecter des informations identifiantes jouent à présent un rôle central dans l'application des règles protectrices édictées, en raison du principe de responsabilisation issu du nouveau cadre européen. La modification du régime protecteur par le RGPD ne remet pourtant pas en cause la spécificité du cadre juridique, fondée sur le recours à une autorité administrative indépendante, relais autonome des pouvoirs publics dans l'application du cadre protecteur. En effet, l'importance de cette autorité n'est pas remise en question par le Règlement qui procède simplement à un ajustement de ses missions, au regard notamment de l'évolution des formalités de mise en œuvre d'un traitement. Aussi, si l'on a renforcé le rôle du délégué à la protection des données, la CNIL et les autorités européennes de protection n'en conservent pas moins une place centrale dans le dispositif.

La loi Informatique et Libertés de 1978 visait à l'origine à protéger les individus contre les traitements réalisés par les administrations. Cette loi a fait l'objet de modifications lui permettant également d'assurer une protection des individus contre les traitements réalisés par des entreprises. Prenant en compte ce changement d'orientation, la transposition de la directive 95/46/CE par la loi du 6 août 2004 est venue renforcer les pouvoirs de la CNIL, tout en limitant ses pouvoirs de contrôle *a priori*. Différents textes ont, en adéquation avec les évolutions technologiques impactant à la fois le nombre de traitements mis en œuvre mais également le nombre de données traitées, procédé à un renforcement nécessaire et progressif des pouvoirs

de contrôle et de sanction de l'autorité administrative indépendante[1141]. Le RGPD s'inscrit résolument dans cette logique, comme en témoigne l'élévation significative du montant des amendes pouvant être prononcées. Surtout, « avec l'allègement des formalités prévues par le RGPD, la CNIL va pouvoir se libérer d'une charge administrative considérable et se repositionner sur sa mission de contrôle *a posteriori* »[1142].

591. Dans le cas français, la CNIL n'a pendant longtemps bénéficié que d'un rôle répressif limité[1143]. Aussi, l'impact des nouvelles technologies a-t-il été double à son égard : d'une part, son rôle de conseil a progressivement été étendu, afin d'aiguiller les responsables de traitements quant à la mise en œuvre de traitements respectueux de la réglementation. D'autre part, elle a progressivement proposé une doctrine importante permettant l'interprétation du cadre juridique, à l'aune des nouvelles techniques de traitement. *Cloud-computing*, objets connectés ou multiplication des transferts internationaux de données sont autant d'éléments dont la CNIL s'est saisie afin d'y apporter des précisions. L'article 57 du Règlement général, dans le prolongement de l'article 11 de la loi Informatique et Libertés[1144], précise cette fonction en indiquant que chaque autorité de contrôle favorise la sensibilisation à la fois du public, mais également des responsables de traitements et des sous-traitants, au regard des évolutions dans le domaine des technologies de l'information et de la communication.

593. Ce rôle de conseiller des autorités administratives de contrôle, qui se manifeste également à l'égard des pouvoirs publics, participe ainsi à la création d'un droit souple de la protection des données à caractère personnel[1145]. Ce recours au droit souple, justifié par la spécialisation croissante des nouvelles technologies et par la complexité des instruments utilisés pour la collecte de données identifiantes, à l'image des dispositifs employés dans le cadre du *quantified-self*, trouve un écho

[1141] La loi du 6 août 2004 a ainsi permis à la Commission de prononcer des amendes proportionnelles à la gravité du manquement constaté, de 150 000 euros à 300 000 euros ou 5% du chiffre d'affaires. La loi pour une République numérique du 7 octobre 2016 a fait passer ce plafond de 150 000 euros à 3 millions d'euros.
[1142] Raouf Saada, « Plaintes et contrôles sur place : analyse de l'activité de la CNIL et enjeux pour l'avenir », *Dalloz IP/IT*, 2018, p. 217.
[1143] David Forest, « Pouvoirs de sanction de la CNIL : le réveil soudain de la belle endormie », *Recueil Dalloz*, 2007, p. 94.
[1144] Celui-ci indique dans un 4° e) que la CNIL « conduit une réflexion sur les problèmes éthiques et les questions de société soulevées par l'évolution des technologies numériques ».
[1145] Conseil d'Etat, *Le droit souple*, Etude annuelle 2013, La Documentation Française, 2012, p. 61.

particulier au niveau européen par le rôle similaire conféré au G29. Cette nouvelle forme de régulation est soutenue par le développement progressif d'agences autonomes et indépendantes. Celles-ci, de nature publique ou privée, participent également à la création d'une nouvelle forme de régulation en contribuant à l'interprétation et à la construction de normes adaptées aux outils techniques utilisés. Enfin, au regard de la rapidité des évolutions technologiques, les questions relatives à la protection des données font également l'objet de différentes études et rapports qui participent à la création de normes d'usages et de bonnes pratiques. Ces différents éléments permettent la mise en œuvre de nouvelles modalités de protection **(Section 1)** et ils conduisent également à un nouveau partage du contentieux **(Section 2)**.

SECTION I – LES NOUVELLES MODALITÉS DE PROTECTION

594. Les règles protectrices des données à caractère personnel, larges dans leur portée et soumises à un principe de neutralité technologique, n'ont pas vocation à s'appliquer à une technologie et à une technique précise mais à une opération de traitement appréciée de manière abstraite. L'absence de toute référence à des procédés techniques dans la législation permet donc l'applicabilité concrète de la réglementation. Pourtant, afin de faire coïncider au mieux ces règles aux nouvelles technologies, celles-ci nécessitent parfois de faire l'objet d'interprétations eu égard aux spécificités de chacun des instruments employés. Ces derniers impliquent donc que des précisions soient apportées, à l'image de celles qui ont pu être apportées au cas des objets connectés et du *quantified-self*. Délivrées par une pluralité d'acteurs aux statuts divers, ces précisions contribuent dès lors à la création d'une nouvelle forme de régulation des données à caractère personnel **(Paragraphe 1)**, qui repose sur une évaluation et une approche par les risques des dispositifs employés **(Paragraphe 2)**.

§1. Une nouvelle forme de régulation

595. La spécificité du droit à la protection des données à caractère personnel, par sa technicité et le caractère évolutif des éléments et objets à réglementer, implique la mise en œuvre d'une nouvelle forme de régulation, fondée sur une doctrine fournie émanant d'acteurs de plus en plus nombreux. En effet, la complexification des questions relatives au numérique, particulièrement prégnante concernant les modalités renouvelées de collecte et de traitement permises par les objets connectés, justifie le recours à des structures nouvelles, relais sectoriels de l'administration[1146], qui vont proposer des solutions plus précises quant à l'application de la règlementation et contribuer à la mise en œuvre de codes de conduites, de packs de conformité ou de référentiels permettant d'expliciter les principes généraux apportées par les textes nationaux et européens. La mise en œuvre

[1146] Jacques Chevallier, *Science Administrative*, PUF, coll. « Thémis », 2019, p. 325.

de cette régulation complète l'ensemble normatif étatique afin de permettre la diffusion d'une culture de la protection des données à caractère personnel[1147].

596. Cette diffusion, qui « se traduit par la diversification croissante des structures administratives »[1148], a donné naissance à un certain nombre d'agences. « Conçues comme le vecteur d'expérimentation d'un modèle administratif fondé sur des valeurs nouvelles », elles témoignent « d'une volonté de faire face à un problème, de répondre à une demande sociale, mieux que ne pourrait le faire une administration classique, engoncée dans la routine bureaucratique » car « qui dit agence, dit aussi flexibilité, réactivité, adaptabilité »[1149]. Phénomène conceptualisé sous l'influence du « *New Public Management* » ou « Nouvelle gestion publique », cette « agencification »[1150] de l'Etat tend notamment à appliquer au secteur public les méthodes du secteur privé et à déléguer la mise en œuvre de politiques publiques à des agences autonomes[1151]. L'agencification s'inscrit dans une transformation progressive du modèle étatique et du processus normatif, caractéristique des sociétés contemporaines qui semblent « être entrées dans une phase nouvelle, dans une large mesure liée au développement technologique »[1152]. Cette transformation des mécanismes régulateurs est ainsi liée au fait que « tout se passe comme si une société nouvelle était en passe d'émerger, la numérisation remettant en cause l'ensemble des équilibres économiques, sociaux et politiques, à travers une véritable rupture »[1153].

La diffusion d'une culture de la protection des données à caractère personnel était traditionnellement l'apanage des autorités administratives indépendantes françaises et européennes **(A)** mais le nombre d'acteurs de nature variée et participant à la mise en œuvre de cette régulation s'est considérablement accru ces dernières années **(B)**.

[1147] Nathalie Métallinos, « Maîtriser le risque Informatique et Libertés », *Droit social*, 2006, p. 378.
[1148] Jacques Chevallier, *L'Etat post-moderne*, 4ème édition, LGDJ, décembre 2017, p. 106.
[1149] *Ibid.*, p. 120.
[1150] Voir par exemple : Caroline Braud, « La notion d' « agence » en France : réalité juridique ou mode administrative ? », *Les Petites Affiches*, 30 août 1995, n° 104, p. 4.
[1151] Conseil d'Etat, *Les agences : une nouvelle gestion publique*, Etude Annuelle 2012, La Documentation Française, 2012, p. 35.
[1152] Jacques Chevallier, *op. cit.*, p. 14.
[1153] *Ibid.*

A. Les autorités administratives indépendantes

597. L'informatique « a révélé un problème latent qui lui préexistait tout en lui donnant des dimensions nouvelles »[1154] et les capacités de traitement qu'elle permet ont justifié dans le courant des années 70 la création d'un cadre juridique protecteur. Révélé par le quotidien *Le Monde*, le projet SAFARI d'interconnexion des fichiers nominatifs de l'administration française a été le point de départ en France d'une réflexion menée sur les impacts de l'informatique et des traitements de données sur les libertés individuelles. Dès 1974, le gouvernement demandait à une Commission spécialement créée de « lui proposer des mesures tendant à garantir que le développement de l'Informatique dans les secteurs public, semi-public et privé se [réaliserait] dans le respect de la vie privée, des libertés individuelles et des libertés publiques »[1155]. Un mécanisme centralisateur des opérations de traitements a été instauré avec la Commission Nationale de l'Informatique et des Libertés, sorte de « conscience nationale des utilisateurs de traitements informatisés »[1156], dont le champ d'action a progressivement été élargi, au gré de l'évolution de la notion de données à caractère personnel[1157]. La démarche du législateur, par la création de la première autorité administrative indépendante, était inédite à l'époque **(1)** et la globalisation du recours à l'informatique et aux traitements de données a justifié, à la suite de l'adoption de la directive de 1995, la création d'un organe européen consultatif **(2)**.

1. L'exemple français

598. L'indépendance de la CNIL. Le législateur français a adopté en 1978 une démarche à la fois classique et originale, « classique puisqu'il a édicté un certain nombre de règles, originale puisqu'il a créé une autorité administrative indépendante chargée d'assurer l'application de la loi »[1158]. La loi du 6 janvier 1978 créant la CNIL utilise en effet pour la première fois les termes d'autorité administrative

[1154] OCDE, *Questions d'ordre politique soulevées par la protection des données et des libertés individuelles*, 1976, p. 177.
[1155] Journal Officiel de la République Française, 1ère séance du mardi 4 octobre 1977, Première session ordinaire de 1977-1978, Débats parlementaires, Assemblée Nationale, Mercredi 5 octobre 1977, p. 5783.
[1156] Commission « Informatique et Libertés », Rapport (« dit rapport Tricot »), *La Documentation Française*, 27 juin 1975, p. 153.
[1157] Tiphaine Bessière, « Loi informatique et libertés : la CNIL veille », *JS*, 2011, n°111, p. 20.

indépendante, « sorte de mandataire légal des citoyens dans leur défense de leurs libertés individuelles ou publiques et de leur droit au respect de leur identité, de leur vie privée »[1159]. On peut ainsi voir à travers ce mécanisme « la grande habileté du droit public français à protéger les libertés en suscitant au sein de l'administration des instances indépendantes suivant la tradition magistralement inaugurée par le Conseil d'Etat en l'an VIII, plutôt qu'en renforçant l'autorité judiciaire »[1160]. Dès lors, et bien que seul le juge la contrôle, la CNIL se « situe dans l'Etat mais ne relève ni du pouvoir hiérarchique, ni du pouvoir de tutelle »[1161]. De cette indépendance propre à la CNIL a découlé l'étendue de ses missions. En effet, celle-ci « se renseigne, réfléchit, conseille, propose, contrôle ; elle informe l'opinion, elle dispose de certains pouvoirs mais surtout, elle aide les autres organes de l'Etat à exercer les leurs »[1162]. La diversité des instruments mis à la disposition de la CNIL permet ainsi sa participation à la création de normes protectrices des données à caractère personnel.

599. L'influence sur la création des normes. La CNIL dispose d'abord d'un pouvoir réglementaire. Celle-ci établit non seulement son règlement intérieur[1163] mais elle édicte également des règlements types en matière de sécurité des systèmes d'information[1164], bien que cette éventualité lui ait parfois paru peu adaptée[1165]. Outre un pouvoir réglementaire propre, la CNIL participe également de façon indirecte à celui-ci en vertu de son pouvoir consultatif. Elle est à ce titre « consultée sur tout projet de loi ou de décret ou toute disposition de projet de loi ou de décret relatifs à la protection des données à caractère personnel ou au traitement de telles données »[1166]. Par ailleurs, elle dispose de la faculté de proposer au gouvernement des mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques.

[1158] Pierre-Alain Weil, « Bilan de la CNIL », *Culture Technique*, n°21, Juillet 1990, p. 186.
[1159] *Ibid.*
[1160] Blandine Barret-Kriegel, *L'Etat et la démocratie*, rapport à François Mitterand, président de la République française, La Documentation française, mars 1986, p. 83.
[1161] Herbert Maisl, « Etat de la législation française et tendance de la jurisprudence relatives à la protection des données personnelles », *Revue Internationale de droit comparé*, 39-3, 1987, pp. 559-580.
[1162] Bernard Tricot, *op. cit.*, p. 153.
[1163] L'article 12 de la loi 78-17 du 6 janvier 1978 modifiée en 2018 indique que « le règlement intérieur de la commission précise notamment les règles relatives aux délibérations, à l'instruction des dossiers et à leur présentation devant la commission, ainsi que les modalités de mise en œuvre de la procédure de labellisation prévue au c du 3° de l'article 11 ».
[1164] Article 8, I, 2, c) de la loi 78-17 du 6 janvier 1978 modifiée en 2018.

Relais juridique permettant l'application concrète de la réglementation, la CNIL est également un relais technique permettant l'évolution de celle-ci puisque, selon les termes de la loi, « elle conduit une réflexion sur les problèmes éthiques et les questions de société soulevées par l'évolution des technologies numériques ». La CNIL rend ainsi des avis motivés sur les différents textes qui lui sont soumis, à l'image de celui rendu le 30 novembre 2017 sur le projet de loi relatif à la protection des données personnelles[1167]. Celle-ci ne rend généralement pas d'avis directement défavorables, mais elle formule des remarques susceptibles d'influencer les pouvoirs publics.

600. L'influence sur l'interprétation des normes. La CNIL peut, pour l'accomplissement de ses missions, adopter des recommandations dans des domaines variés, recommandations qui sont susceptibles d'influencer l'interprétation et la pratique de la réglementation relative à la protection des données à caractère personnel. Cette autorité administrative se fait donc le relais de la législation en proposant une interprétation concrète des dispositions législatives. A ce titre, il est possible d'observer à propos des autorités administratives indépendantes que « c'est par des voies extra juridiques que celles-ci exercent le plus volontiers leur action et sans doute parviennent aux meilleurs résultats. S'efforçant de convaincre, plutôt que d'imposer, elles multiplient les démarches, les conciliations, les recommandations »[1168]. Ce qui peut être qualifié de « déontologie de la CNIL »[1169] semble justifié au regard des évolutions technologiques permises par le numérique et à la spécificité de chacun des moyens de traitement employés. Ainsi, la CNIL, émanation de l'Etat dont l'action est soumise au seul contrôle du Conseil d'Etat et de la Cour des comptes, s'inscrit dans un édifice juridique original. Celui-ci, « dont le but est d'organiser des procédures de décision et des moyens de maintenir l'équilibre entre les prérogatives de la puissance publique et des libertés dont il faut garantir

---

[1165] Herbert Maisl, art. précité, p. 563.
[1166] Article 8, 4°, a) de la loi 78-17 du 6 janvier 1978 modifiée en 2018.
[1167] CNIL, Délibération n°2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du 6 janvier 1978.
[1168] François Gazier, Yves Cannac, *Etude sur les autorités administratives indépendantes*, La documentation Française, coll. « Etudes et documents du Conseil d'Etat », n°35, 1983-1984, p. 22.
[1169] Herbert Maisl, art. précité, p. 565.

l'exercice »[1170], permet le développement d'une régulation qui cherche à concilier innovation et protection des libertés.

Le recours au droit souple, favorisé par le législateur lui-même, est aujourd'hui l'instrument privilégié de la régulation. Mais la spécificité de ce droit, qui se caractérise notamment par sa souplesse, pourrait être amenée à s'estomper. En effet, le Conseil d'Etat a récemment ouvert la voie du recours pour excès de pouvoir à l'encontre des actes de droit souple adoptés par les autorités de régulation[1171]. Confirmée depuis[1172], cette solution nécessite pour être retenue de s'attacher aux effets notables de l'acte ou à son influence significative : même en l'absence d'effets, l'acte est susceptible d'un recours si son objet ou sa finalité est d'influer sur le comportement de ses destinataires[1173]. Selon ces critères, les instruments de droit souple mis à disposition de la CNIL par l'article 1er de la loi du 20 juin 2018 – lignes directrices, recommandations, référentiels ou codes de bonne conduite – pourraient désormais faire l'objet d'un recours pour excès de pouvoir. Cette solution, révélatrice de la consécration progressive du droit souple en tant que source du droit et de son assimilation éventuelle aux règles de droit « dur »[1174], témoigne de son opposabilité. Mais la portée de cette solution à l'égard des instruments de droit souple employés par la CNIL fait encore l'objet d'incertitudes. En effet, la solution retenue par le Conseil d'Etat semble avoir vocation à s'appliquer uniquement aux autorités de régulation[1175]. Or la CNIL n'est pas une autorité de régulation au sens strict. Il faudrait dès lors revenir à la distinction courante entre les autorités indépendantes « exerçant une mission de régulation économique et celles chargées de protéger les droits et libertés fondamentaux »[1176].

[1170] CNIL, *Premier rapport au Président de la République et au Parlement*, Bilan et perspectives, 1978-1980, La Documentation Française, Paris, 1980, p. 15.
[1171] CE, ass., 21 mars 2016, n° 368082 (Lebon 76 avec les concl. ; *AJDA* 2016. 572 ; *ibid*. 717, chron. L. Dutheillet de Lamothe et G. Odinet ; D. 2016. 715, obs. M.-C. de Montecler ; *AJCA* 2016. 302, obs. S. Pelé ; Rev. sociétés 2016. 608, note O. Dexant - de Bailliencourt ; *RFDA* 2016. 497, concl. S. von Coester ; *RTD civ*. 2016. 571, obs. P. Deumier ; *RTD com*. 2016. 298, obs. N. Rontchevsky ; *ibid*. 711, obs. F. Lombard) ; CE, ass., 21 mars 2016, n° 390023 (Lebon 88 avec les concl. ; *AJDA* 2016. 572 ; *ibid*. 717, chron. L. Dutheillet de Lamothe et G. Odinet ; D. 2017. 881, obs. D. Ferrier ; *AJCA* 2016. 302 ; Rev. sociétés 2016. 608, note O. Dexant - de Bailliencourt ; *RFDA* 2016. 506, concl. V. Daumas ; *RTD civ*. 2016. 571, obs. P. Deumier ; *RTD com*. 2016. 711, obs. F. Lombard).
[1172] CE, sect., 13 juill. 2016, n° 388150, *Société GDF-Suez*, Lebon ; *AJDA*, 2016. 2119, note F. Melleray.
[1173] Christophe Testard, « Le droit souple, une « petite » source canalisée », *AJDA*, 2019, p. 934.
[1174] *Ibid*.
[1175] Fabrice Melleray, « Le contrôle juridictionnel des actes de droit souple », *RFDA*, 2016, p. 679.
[1176] Patrice Gélard, Office d'évaluation de la législation, *Rapport sur les autorités administratives indépendantes*, 2006, tome 1, p. 42.

Dotée d'un statut original pour l'époque, la CNIL est initialement « chargée autant, sinon plus, d'informer que de contraindre »[1177]. Son indépendance, garantie de son efficacité et dont l'effectivité est assurée autant par la désignation de ses membres[1178] que par son mode de financement, lui permet en tant que régulateur du secteur de l'informatique de développer une doctrine importante. La CNIL dispose d'un pouvoir réglementaire fortement limité[1179] mais elle participe effectivement à la création et au développement d'un droit souple de la protection des données à caractère personnel. Les avis[1180], recommandations et prises de positions publiques dont elle est à l'origine, s'ils ne lient pas les pouvoirs publics[1181], contribuent ainsi à la mise en œuvre d'un ensemble de bonnes pratiques favorisant le développement vertueux de la technologie. Elle a ainsi permis à la loi Informatique et Libertés de 1978 de rester pertinente dans son principe, au regard des différentes innovations technologiques qui ont vu le jour depuis son adoption. Celle-ci continue, après l'adoption du RGPD, de proposer une doctrine importante, à l'image des packs de conformité qu'elle édite à destination des responsables de traitement. Aussi, bénéficie-t-elle, depuis l'adoption de la directive 95/46/CE, d'un important relais au niveau européen.

2. Le cas particulier du « groupe de l'article 29 »

601. La généralisation du recours aux AAI en Europe. La création d'une autorité administrative indépendante dédiée au respect des libertés par l'informatique était en France, en 1978, une innovation juridique. Mais d'autres Etats avaient déjà procédé à l'établissement d'autorités qui devaient autoriser, en amont, la mise en œuvre de traitements de données à caractère personnel. L'autorité suédoise de protection des données à caractère personnel, *Datainspektionen*, a par exemple été

[1177] Jacques Thyraud, *Rapport fait au nom de la Commission des Lois constitutionnelles, de Législation, du Suffrage universel, du Règlement et d'Administration générale, sur le projet de loi adopté par l'Assemblée Nationale, relatif à l'informatique et aux libertés*, Sénat, Première Session Ordinaire de 1977-1978, n° 72, p. 25.
[1178] La CNIL est composée de 18 membres (6 représentants des hautes juridictions, 5 personnalités qualifiées, 4 parlementaires, 2 membres du Conseil économique, social et environnemental, 1 membre de la Commission d'accès aux documents administratifs) élus ou désignés par les assemblées ou les juridictions auxquelles ils appartiennent, par le Premier ministre et les présidents des deux assemblées.
[1179] Philippe Luppi, « L'unité du pouvoir réglementaire du Premier ministre et son caractère ab initio », *AJDA*, 2007, p. 1643.
[1180] Avis que le Conseil d'Etat qualifie de consultatif et ne pouvant avoir valeur d'avis conformes, voir notamment : CE, 26 juillet 1996, n° 160481, mentionné aux tables du recueil Lebon.
[1181] Conseil Constitutionnel, 14 décembre 2006, n° 2006-544 DC, *Loi de financement de la sécurité sociale pour 2007*.

créée à la suite de l'adoption, le 11 mai 1973, de la première réglementation nationale relative à la protection des données (*Datalagen*). Malgré le phénomène de globalisation du droit à la protection des données à caractère personnel, matérialisé par l'élaboration de lignes directrices sur la protection de la vie privée par l'OCDE[1182] et par l'adoption de la Convention 108 du Conseil de l'Europe[1183], il faudra attendre l'adoption de la directive 95/46/CE pour procéder à la création d'autres autorités de protection des données. En effet, la directive précisait, dans son article 28, que chaque Etat membre devait prévoir l'existence d'une ou plusieurs autorités publiques indépendantes chargées de surveiller l'application des dispositions de la directive sur son territoire.

602. La création d'un organe regroupant les représentants des AAI. La directive a procédé, dans le même temps, à la création d'un « groupe de protection des personnes à l'égard du traitement des données à caractère personnel ». Ce groupe au caractère simplement consultatif, qui n'était pas une autorité administrative indépendante, se composait d'un représentant de chacune des autorités de contrôle nationales. Ces missions étaient théoriquement similaires à celles des autorités nationales mais celui-ci ne disposait pas de pouvoir réglementaire, excepté celui de pouvoir établir lui-même son règlement intérieur. Le G29 a d'abord eu un rôle de conseil à l'égard de la Commission européenne, avec la mission de contribuer à l'application homogène de la directive[1184]. Mais il a pu progressivement émettre, de sa propre initiative, des recommandations sur toute question concernant la protection des personnes à l'égard du traitement de données à caractère personnel dans la communauté. Le G29 a ainsi également procédé au développement d'un droit souple, à l'image de celui dégagé par la CNIL. Celui-ci a cependant présenté un spectre plus large, en raison de sa portée territoriale et du consensus existant entre les différentes autorités nationales de protection[1185].

[1182] OCDE, Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, adoptées le 23 septembre 1980
[1183] Conseil de l'Europe, Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 janvier 1981.
[1184] Le groupe de l'article 29 contribue ainsi au maintien effectif de la notion de « protection adéquat » qui est présumée lorsqu'un transfert de données à caractère personnel a lieu entre Etats appartenant à la Communauté européenne.
[1185] G 29, *5ème rapport annuel pour l'année 2000*, WP54, p. 3.

603. Un acteur majeur de la protection des données. Conçu à l'origine comme un organe consultatif, le groupe de l'article 29 « s'est progressivement transformé en acteur majeur de la protection des données sur le plan européen mais aussi mondial »[1186]. Son rôle de conseiller a peu à peu évolué pour appréhender des questions aussi bien juridiques que techniques, en adéquation avec la consécration progressive d'un droit fondamental de la protection des données dans l'Union européenne[1187]. La complexité croissante des dispositifs utilisés pour les traitements de données ainsi que l'amplification des transferts internationaux de données ont entrainé une nécessaire modification de la raison d'être du G29. Les autorités de protection des données européennes ont dès lors dû être en mesure de « mener des expertises techniques approfondies et documentées afin de rédiger des avis pointus et opérationnels », les contributions de groupe de l'article 29 permettant de « clarifier la réglementation » [1188] et dès lors d'interpréter celle-ci au regard du développement de nouvelles technologies, telles que les objets connectés et le *quantified-self*[1189]. La portée des avis et recommandations du groupe s'est ainsi élargie, visant non seulement les institutions européennes mais également directement les responsables de traitement et les personnes concernées par de tels traitements.

604. La contribution à la création du droit souple. Le caractère consultatif du groupe de l'article 29 fait que ses décisions n'ont en théorie pas de valeur contraignante. Pourtant, celui-ci a contribué au développement d'un droit souple d'origine institutionnelle avec des documents faisant généralement autorité[1190]. A l'image du travail réalisé par la CNIL au niveau national et de son influence certaine sur la législation, le G29 a contribué à l'évolution du droit de la protection des données à caractère personnel au niveau européen. De façon plus large, il a influencé les législations et les juridictions nationales[1191], le travail réalisé par le groupe étant souvent repris par les autorités de contrôle nationales. Celui-ci a ainsi contribué au

[1186] Sophie Nerbonne, « Le Groupe de l'article 29 est-il en mesure de s'imposer comme le régulateur des régulateurs par ses prises de position ? », *Legicom*, n° 42, 2009, p. 37 à 46.
[1187] *Ibid.*, p. 39.
[1188] *Ibid.*, p. 40.
[1189] Voir par exemple l'avis adopté le 16 septembre 2014 par le Groupe de l'article 29 sur le développement de l'Internet des objets.
[1190] Anne Debet, Jean Massot, Nathalie Metallinos, *op. cit.*, p. 185.
[1191] Voir par exemple : TGI Paris, 28 janvier 2014, *M. X c/. Google Inc. et Google France* sur l'interprétation de la notion de « moyens » au regard de l'avis 1/2008 sur les moteurs de recherche.

développement d'un « mécanisme de gouvernance réflexive permettant une coopération trans-gouvernementale »[1192]. Le G29 a également pu influencer les prises de position du Contrôleur européen à la protection des données, institution chargée de vérifier la légalité des traitements réalisés par les institutions de l'Union européenne, contribuant ainsi au développement d'une politique unifiée en la matière.

605. Le Comité européen de la protection des données. Le G29 a disparu avec l'entrée en application du RGPD. Ce dernier instaure un Comité européen de la protection des données au rôle similaire et dont les missions sont présentées à l'article 70 du texte[1193]. Reprenant les attributions du groupe de l'article 29, ce Comité bénéficie de pouvoirs renforcés, notamment concernant les traitements transnationaux. Le considérant 136 mentionne explicitement que « le comité devrait également être habilité à adopter des décisions juridiquement contraignantes en cas de litiges entre autorités de contrôle ». Ces décisions sont susceptibles d'être contestées puisque le considérant 143 précise que « toute personne physique ou morale a le droit de former un recours en annulation des décisions du comité devant la Cour de justice ».

Le G29 a contribué, depuis 1995, à l'élaboration d'une doctrine importante sur l'application du cadre juridique aux nouvelles technologies et le Comité européen de la protection des données a vocation à poursuivre le travail réalisé. Parallèlement à ces institutions, de nombreuses agences spécialisées se sont développées et elles influencent également la création et pratique du droit à la protection des données à caractère personnel.

B. Le cas des agences autonomes

606. La complexité croissante des technologies du numérique a entraîné la superposition de différentes strates ou différentes couches de problématiques techniques : prospection commerciale fondée sur l'exploitation de données à caractère

[1192] TGI Paris, 28 janvier 2014, *M. X c/. Google Inc. et Google France.*
[1193] Celui-ci est notamment chargé de surveiller et garantir la bonne application du Règlement, de conseiller la Commission sur toute question relative à la protection des données à caractère personnel dans l'Union ou encore de publier des lignes directrices, recommandations et bonnes pratiques dans différents domaines touchant à la question de la protection des données à caractère personnel.

personnel, transferts internationaux croissants d'informations, développement du *cloud*, applications de santé mobile ou encore déploiement d'objets connectés dans le cadre du *quantified-self*. Ces différents éléments, qui contribuent plus généralement à la transformation numérique de la société et plus globalement, de l'action publique, ont progressivement entraîné la création d'agences spécialisées aux statuts divers. La CNIL ou encore le groupe de l'article 29 ont déjà proposé des documents relatifs à ces évolutions du numérique et à leur prise en compte par la réglementation. Mais des instances nouvelles ont progressivement vu le jour, proposant également leur interprétation de la législation en participant ainsi à la régulation du secteur. Objet « juridico administratif en construction » [1194], la notion d'agence englobe des structures administratives très diverses qui participent au renouvellement de la gestion publique. Celles-ci se caractérisent en tout état de cause par leur diversité **(1)** mais également par la souplesse des mesures qu'elles proposent **(2)**.

1. La diversité des agences

607. La définition juridique. La définition juridique d'agence reste encore aujourd'hui difficile à déterminer. Le Conseil d'Etat, dans son étude annuelle de 2012 consacrée aux agences, relève que les « catégories juridiques ne sont ici d'aucun secours »[1195] en raison de la diversité des formes que peuvent prendre ces agences et qui rend leur identification complexe. Tout au plus, peut-on les identifier à travers la présence de deux critères cumulatifs : l'un relatif à l'autonomie dont elles disposent et l'autre, relatif à l'exercice d'une responsabilité structurante dont elles ont la charge dans la mise en œuvre d'une politique publique nationale. Ainsi, l'agence est autonome en ce que le pouvoir exécutif n'a pas vocation à intervenir dans sa gestion courante même s'il définit les orientations politiques que celle-ci doit mettre en œuvre[1196].

Selon la définition retenue par le Conseil d'Etat, deux agences sont particulièrement susceptibles de contribuer à la régulation à apporter aux objets

[1194] Jean-Marc Sauvé, *Les agences : une nouvelle gestion publique*, Introduction lors du colloque organisé par le Conseil d'Etat le 19 octobre 2012.
[1195] Conseil d'Etat, *Les agences : une nouvelle gestion publique*, Etude Annuelle 2012, La Documentation Française, 2012, p. 12.

connectés et à l'automesure : l'Agence nationale de sécurité du médicament et des produits de santé (ANSM) et l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Mais, le développement croissant du numérique, son impact sur les politiques publiques ainsi que sur les droits fondamentaux des individus a rapidement entraîné la création d'autres organismes spécialisés, ne répondant pas exactement à la définition juridique proposée par le Conseil d'Etat.

608. Les agences peuvent être créées *ad hoc*[1197]. Mais d'autres procédés existent pour parvenir à leur création : certains organismes instaurent en leur sein des groupes spécialisés sur des sujets particuliers[1198] et d'autres structures peuvent décider de se regrouper[1199]. D'origine gouvernementale, académique ou privée, ces institutions ont toutes pour particularité de participer indirectement à la régulation du domaine des traitements de données à caractère personnel. La diffusion de la doctrine et du droit souple des institutions de contrôle nationales et européennes de protection est ainsi appuyée par ces agences. Dès lors, en reprenant les positions institutionnelles et en les adressant à des professionnels du secteur, concepteurs et développeurs d'applications ou d'objets connectés, ces agences permettent une diffusion des principes protecteurs des données. Le sous-groupe « Quantified-self » du groupe de travail « Données de santé » de l'Association française des correspondants à la protection des données à caractère personnel (AFCDP) a par exemple repris, dans la synthèse de ses travaux, la définition de donnée relative à la santé proposée par la CNIL dans son « Pack de conformité – logement social » de 2014 ainsi que les critères d'identification (données médicales, données brutes et conclusions relatives à l'état de santé) proposés en 2015 par le groupe de l'article 29. L'action des agences est particulièrement importante en matière de *quantified-self*. Elles contribuent tout d'abord à faire évoluer la réglementation. Mais elles permettent

---

[1196] *Ibid.*
[1197] Conseil National du Numérique, commission consultative créée le 29 avril 2011 par le décret n° 2011-476.
[1198] Groupe de travail « Données de santé » et sous-groupe « Quantified-self » de l'Association française des correspondants à la protection des données à caractère personnel.
[1199] Groupe de travail 28 (GT28) du Comité stratégique de filière (CSF) santé et qui regroupe notamment la Délégation à la Stratégie des Systèmes d'Information de Santé du ministère des Affaires sociales et de la Santé, le ministère de l'Economie, de l'Industrie et du Numérique, et les Fédérations d'industriels regroupés au sein de l'alliance eHealth France.

également d'identifier certains enjeux relatifs à la santé et au développement économique.

609. Le Conseil national du Numérique. Le Conseil national du Numérique (CNNum) dispose d'un rôle particulier sur l'échiquier des organismes traitant de la question de l'innovation technologique. Commission consultative créée en avril 2011, composée de dix-huit membres choisis en raison de leurs compétences dans le domaine de l'économie numérique, le CNNum a pour mission « d'éclairer le gouvernement et de participer au débat public dans le domaine du numérique » et peut être à cette fin « consulté par le gouvernement sur tout projet de disposition législative ou réglementaire susceptible d'avoir un impact sur l'économie numérique »[1200]. Celui-ci peut également formuler des recommandations et aiguiller les pouvoirs publics quant aux dispositions et mesures à adopter. Par exemple, faisant écho au concept d'autodétermination informationnelle, le CNNum anticipait dans un rapport l'application des mesures adoptées par le RGPD en recommandant de mieux encadrer le recueil du consentement, de créer une action collective pour les individus ou encore, de mettre en œuvre un droit à la portabilité des données[1201].

Le rôle du CNNum doit cependant être distingué de celui de la CNIL, étant donné qu'il ne dispose d'aucun pouvoir règlementaire ni d'aucuns moyens de contrôle. Pourtant, son influence sur les droits et libertés des individus est aisément perceptible. Dans son avis rendu sur le projet de loi pour une République numérique, il a par exemple recommandé le renforcement du droit à la portabilité des données et soutenu la consécration du principe de libre disposition des données. Il s'est prononcé en faveur d'une « approche personnaliste de la protection des données », celles-ci devant être considérées comme des émanations de la personne et non comme des biens susceptibles d'appropriation[1202]. Son rayonnement s'est manifesté à travers son intervention dans la renégociation de l'accord *Privacy Shield* sur la protection des

[1200] Anthony Astaix, « Internet : le Conseil national du numérique (re)devient une réalité », *Dalloz Actualité*, 4 mai 2011.
[1201] Conseil national du Numérique, *La santé, bien commun de la société numérique*, octobre 2015, p. 23.
[1202] Conseil national du numérique, Avis n° 2015-3 relatif au projet de loi pour une République numérique, 30 novembre 2015, p. 2 et p. 7.

données, au regard du manque de garanties apportées au cas de la surveillance généralisée[1203].

610. L'Agence nationale de sécurité du médicament et des produits de santé. Le CNnum proposait déjà, dans son rapport relatif à la santé et au numérique, de « redonner au citoyen la maîtrise de ses données de santé » en « concrétisant l'*empowerment* individuel et collectif sur données »[1204]. Mais d'autres agences, spécialisées sur les questions de santé, participent également à la régulation des dispositifs d'automesure. L'Agence nationale de sécurité du médicament et des produits de santé (ANSM) contribue ainsi, par ses travaux, à la transposition concrète des mesures législatives et réglementaires à destination des concepteurs d'objets connectés et d'applications. Elle assure notamment l'information des personnes concernées, explicitant par exemple la différence entre objet connecté ludique et dispositif médical bénéficiant d'un marquage CE[1205]. D'autres institutions, telles que le Conseil national de l'Ordre des médecins, contribuent aussi à définir les rapports entre *quantified-self* et santé en identifiant les bénéfices que celui peut présenter pour le domaine sanitaire[1206].

611. La « Nouvelle France Industrielle ». L'influence des différentes agences sur la régulation vient également du rapprochement entre entités distinctes et du dialogue qui s'instaure directement avec les opérateurs et les entreprises du numérique. La feuille de route portant sur l'Internet des objets, publiée par le mouvement de développement économique « Nouvelle France Industrielle » (NFI), acte par exemple le rapprochement entre différents acteurs du monde du numérique pour parvenir à de nouvelles solutions techniques permettant le déploiement vertueux d'objets connectées. La Nouvelle France Industrielle, qui compte par exemple le fondateur de la firme Withings parmi ses membres, vise ainsi à étudier « les évolutions en matière de réglementation qui seraient rendues nécessaires pour tenir

[1203] Conseil national du numérique, *Pourquoi le Privacy Shield doit être renégocié*, Communiqué, mardi 19 septembre 2017, disponible en ligne à cette adresse : https://cnnumerique.fr/pourquoi-le-privacy-shield-doit-etre-renegocie.
[1204] Conseil national du Numérique, *La santé, bien commun de la société numérique*, octobre 2015, p. 16.
[1205] ANSM, *Logiciels et applications mobiles en santé*, Point d'information, 5 mai 2015, disponible en ligne à cette adresse : http://ansm.sante.fr/S-informer/Points-d-information-Points-d-information/Logiciels-et-applications-mobiles-en-sante-information-des-utilisateurs-Point-d-information
[1206] Conseil national de l'Ordre des médecins, *Santé Connectée, de la E-santé à la santé connectée*, janvier 2015, p. 12.

compte de l'évolution des réseaux et des usages liés à l'Internet des objets »[1207]. Poursuivant des travaux réalisés notamment par l'Autorité de régulations des communications électroniques[1208] et qui ont eu l'occasion de réunir plusieurs organismes[1209], la NFI contribue à la promotion d'un environnement sécurisé pour le développement des objets connectés. Elle s'appuie sur l'Agence nationale de la sécurité des systèmes d'information, service rattaché au Secrétaire général de la défense et de la sécurité nationale et qui est notamment chargé de la promotion de technologies sécurisées[1210].

Ces différents organismes et groupements contribuent à l'évolution de la régulation en proposant une analyse croisée entre opportunités de développement économique, régulation technologique et évaluation des risques liés à la sécurité. Cette approche sectorielle, tout en contribuant au développement de bonnes pratiques telles qu'elles sont encouragées par le Règlement général européen, se caractérise par la souplesse des mesures instaurées.

2. La souplesse des mesures

612. L'ensemble des rapports et documents de travail proposé par des organismes aux statuts divers s'inscrit dans un mouvement plus général de spécialisation et de décentralisation de la régulation. L'impossibilité de prévoir en amont, par un texte normatif de portée générale, l'ensemble des subtilités techniques permises par l'apparition de nouvelles technologies contribue au développement d'un droit souple composé de bonnes pratiques et de recommandations à destination des opérateurs et entreprises du numérique. Susceptible d'impacter le processus normatif, le propre de cette forme de régulation est d'être en principe dénuée de force contraignante.

613. La nécessité du recours au droit souple. Le Conseil d'Etat, constatant que le droit souple « peut participer du renouvellement de l'Etat en élargissant la

[1207] Nouvelle France Industrielle, *op. cit.*, p. 15.
[1208] ARCEP, *Internet des objets : inventer une régulation pro innovation*, Conférence de l'ARCEP, 7 novembre 2016.
[1209] Voir par exemple : Arcep, Préparer la révolution de l'Internet des objets, Livre Blanc, 7 novembre 2016, p. 2 qui réunit entre autres la CNIL, l'Agence nationale pour la sécurité des systèmes d'information ou la direction générale des entreprises.
[1210] ANSSI, *Référentiel Général de sécurité, Annexe B1, Mécanismes cryptographiques*, 21 février 2014, 63 p.

gamme des moyens d'action dont celui-ci dispose », en propose une définition fondée sur trois critères cumulatifs. Ainsi, le droit souple a pour objet de modifier ou d'orienter les comportements de ses destinataires, il ne crée pas de droits ou d'obligations et enfin, il présente un degré de formalisation et de structuration qui l'apparente aux règles de droit[1211]. Ces trois critères sont remplis par les travaux de la CNIL et du G29. Mais, en participant à la reconfiguration des appareils d'Etat, les agences « ne saurait manquer d'avoir une incidence sur la relation au droit et partant, sur la conception même des phénomènes juridiques »[1212]. Un droit souple en est issu, présentant souvent une grande effectivité car les acteurs concernés se conforment à leurs recommandations[1213]. Les travaux réalisés par les différentes agences et groupements contribueraient ainsi au développement de normes « à fonction directive souple », par opposition aux normes « à fonction directive autoritaire »[1214]. Si pour certains auteurs, « les nouveaux visages de la règle de droit ne corrompent pas son classement dans la catégorie des impératifs »[1215], il faut voir que les règles utiles à la régulation du *quantified-self* et au numérique constituent, plus qu'un « impératif catégorique », un « impératif conditionnel » selon la distinction proposée par Kant[1216].

Dès lors, ce droit souple, qui fonde son efficacité sur le consentement des individus appelés à s'y conformer, permet d'appréhender avec plus d'efficacité les phénomènes émergents[1217]. Surtout, si le droit souple peut accompagner la mise en place de normes législatives, il les préfigure dans certains cas en anticipant l'adoption de règles de droit dur[1218].

614. La consécration par le RGPD. Le RGPD cherche à favoriser le développement de règles susceptibles de répondre au mieux aux considérations spécifiques posées par l'évolution des traitements. Dès lors, il prône le recours à des

[1211] Conseil d'Etat, *Le droit souple*, Etude annuelle 2013, La Documentation Française, 2012, p. 61.
[1212] Jacques Chevallier, *op. cit.*, p. 125.
[1213] Jacky Richard, Laurent Cytermann, « Le droit souple dans la vie de l'entreprise et de la fonction publique : une tension féconde avec le droit dur », *Droit social*, 2014, p. 400.
[1214] Paul Amselek, « Norme et loi », *APD*, T. 25, 1980, pp. 88-121.
[1215] Denys de Béchillon, *Qu'est-ce qu'une règle de droit*, Odile Jacob, 1997, p. 216.
[1216] Valérie Lasserre, Benoït Lecourt, Sarah Cassella (dir.), *Le droit souple démasqué*, Pedone, 2018, 194 p.
[1217] Jacky Richard, Laurent Cytermann, art. précité, p. 400.
[1218] A l'image par exemple des Règles d'entreprise contraignantes développées par le groupe de l'article 29 et reprises par le RGPD.

instruments de droit souple favorisant la conformité, tels que des codes de conduites « développés par des associations ou autres organismes représentant des catégories de responsables du traitement ou de sous-traitants »[1219]. Ces codes de conduite visent à faciliter la bonne application de la règlementation et doivent permettre de répondre au mieux aux spécificités des traitements mis en œuvre. Certaines subtilités nécessitent en effet la mise en œuvre de référentiels plus précis. Mais, si les codes de conduite relèvent du droit souple, le mécanisme de certification qui s'y attache correspond davantage à du « droit dur ». Comme le souligne le Conseil d'Etat, « le fait même de parler de codes de bonne conduite montre qu'un des enjeux du droit souple est de jeter un pont entre l'univers de l'éthique (la bonne conduite) et celui du droit (le code) »[1220]. En effet, le mécanisme d'approbation des codes de conduite mis en œuvre par le RGPD est créateur d'obligations pour les responsables de traitement, l'article 71 instituant une procédure de contrôle du code. Une telle homologation des codes de conduite marque « la possibilité de la transformation d'un instrument de droit souple en règle de droit dur, d'un durcissement du droit souple, sans changement de son contenu »[1221]. Le caractère contraignant conféré par l'homologation en fait finalement des instruments de droit dur, étant donné qu'ils deviennent créateurs d'obligations pour les responsables de traitement. Ceux-ci seraient dès lors plus inspirés du droit souple que véritablement créateur d'un tel droit[1222]. Le recours au terme de « codes de conduite » par le RGPD semble dès lors porteur d'ambiguïtés.

615. La diversité des instruments. Le RGPD favorise le recours à d'autres instruments de droit souple. Le Comité européen de la protection des données est par exemple chargé de publier des lignes directrices, recommandations et bonnes pratiques afin de favoriser le respect de la réglementation. Ces outils s'inscrivent dès lors dans la démarche de conformité qui est prônée et également dans un rapport de complémentarité avec les dispositions du texte. La responsabilisation accrue des responsables de traitements ne doit en effet pas conduire à un recul de l'Etat dans la prise en compte des problématiques relatives au numérique. En effet, un risque

[1219] Considérant 98 du Règlement (UE) 2016/679.
[1220] Conseil d'Etat, *op. cit.*, p. 63.
[1221] *Ibid.*, p. 73.
[1222] Sophie Joissains, *Rapport fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi, adopté par l'Assemblée Nationale après engagement de la procédure accélérée, relatif à la protection des données personnelles*, Sénat, n° 350, 14 mars 2018, p. 198.

d'atomisation des politiques publiques serait susceptible de se réaliser par le recours aux agences et leur multiplication pose à l'Etat la question « de la coordination et du pilotage qu'il doit assurer afin qu'il y'ait une cohérence de l'action publique » [1223]. L'agence ne doit pas être considérée comme un démembrement de l'Etat mais au contraire comme une composante de celui-ci, instrument de son action. En effet, le recours aux agences et la mise en commun des savoirs qu'elle favorise doit permettre une plus grande proximité entre régulateurs et entreprises du numérique.

Les instruments de droit souple établis s'inscrivent dans un dispositif qui procède, pour déterminer l'intensité de la protection à apporter, à une évaluation des risques.

§2. La place de l'évaluation dans le dispositif de protection

616. Le système de protection mis en œuvre par le RGPD repose sur une évaluation des risques que les traitements de données à caractère personnel réalisés sont susceptibles de présenter pour les individus. Cet élément figure explicitement au sein du nouveau texte européen : les mesures de droit souple contribuant à la conformité des traitements réalisés doivent tenir compte du risque qu'ils présentent pour les droits et libertés des personnes physiques[1224]. Le RGPD fait ainsi de la notion de risque et de son intensité le curseur de l'amplitude des mesures protectrices à déployer. Le risque s'entend d'une combinaison entre la probabilité qu'un événement se réalise et ses conséquences. Il peut également provenir de l'écart entre le résultat prévu et celui attendu en ayant, dans certains cas, des conséquences positives[1225]. Le risque fait désormais l'objet d'une évaluation par les responsables de traitement **(A)**, ceux-ci pouvant également avoir recours à des outils de certification afin d'en tempérer la portée **(B)**.

[1223] Anthony Astaix, « Réfléchir aux agences, c'est réfléchir à l'État », *Dalloz Actualité*, 17 septembre 2012.
[1224] Considérants 74 et 75 du Règlement (UE) 2016/679.
[1225] AFNOR, *Management des risques – approche globale*, guide ISO/IEC 73, Recueil Norme et réglementation, Editions Afnor, décembre 2009.

A. L'évaluation par les usages et les pratiques

617. La référence au risque, déjà mentionnée à propos de la sécurité des traitements, est désormais généralisée. Elle devient un critère de mise en œuvre d'instruments de droit souple. Le risque est présenté comme « une situation, un ensemble d'événements dont l'occurrence est incertaine […] et résulte de la conjonction d'un aléa et de la vulnérabilité des enjeux humains, environnementaux ou économiques »[1226]. Les évolutions du cadre juridique sont particulièrement révélatrices de la place croissante du risque dans la législation, le droit de la responsabilité civile[1227] et de la responsabilité administrative[1228] ayant consacré une place importante à la notion. Cette reconnaissance juridique, relativement nouvelle, permet de « contraindre les pouvoirs publics, garants de l'ordre public, à mettre en œuvre des actions de prévention »[1229]. Appliquée au domaine des objets connectés et du *quantified-self,* cette prise en compte en amont des risques devrait permettre de pallier les insuffisances des principes de finalité, de proportionnalité et de durée de conservation limitée. Développée par le RGPD **(1)**, l'approche par les risques entraîne le déploiement d'un dispositif concurrentiel fondé sur la confiance **(2)**.

1. Une approche par les risques

618. La liste des risques. Le RGPD fait dépendre la mise en œuvre de mesures de conformité issues du droit souple du risque que les traitements peuvent faire courir aux individus. Une importante liste des conséquences éventuelles de ce risque est développée par le texte. Ceux-ci peuvent entraîner des « dommages physiques, matériels ou un préjudice moral »[1230] pour les individus, ainsi « 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

[1226] Pierre-Yves Charpentier, « La gestion du risque : de l'approche juridique à l'ébauche d'une méthodologie managériale », *Management & Avenir*, vol. 74, no. 8, 2014, p. 191 à 209.
[1227] Voir par exemple : Franck Verdun, *La gestion des risques juridiques*, Editions d'organisation, Eyrolles, 2006, p. 11.
[1228] Le Conseil d'Etat reconnaît la possibilité d'une responsabilité sans faute et sur le seul fondement du risque dans l'arrêt Cames, 21 juin 1895, Rec. Lebon, p. 509.
[1229] Pierre-Yves Charpentier, article précité, p. 192.

par le secret professionnel ou tout autre dommage économique ou social important »[1231].

De manière générale, le texte précise que ce risque porte sur les droits et libertés des personnes concernées par des traitements de données. L'intensité du risque est également précisée, le cas du « risque élevé » susceptible de se réaliser nécessitant la mise en œuvre d'une analyse d'impact relative à la protection des données ou encore la notification d'une violation de sécurité. Le considérant 76 du texte précise par ailleurs la méthodologie à adopter puisque celui-ci indique qu'il convient de déterminer la probabilité et la gravité du risque pour les droits et libertés de la personne concernée « en fonction de la nature, de la portée, du contexte et des finalités du traitement ».

La notion de risque est omniprésente dans le texte du Règlement. Le terme de « risque » est employé 78 fois dans le RGPD, contre 8 fois pour la directive de 1995 et 4 fois pour la loi Informatique et Libertés de 1978. Le risque irrigue à de nombreux égards les conditions de mise en œuvre d'instruments de conformité directement issus ou inspirés du droit souple. A ce titre, l'une des missions premières du Comité qui remplace le groupe de l'article 29 est de proposer des lignes directrices, des recommandations et des bonnes pratiques qui doivent permettre aux responsables de traitement de limiter les risques pesant sur les individus lorsqu'ils mettent en œuvre des traitements de données. Cette prévention du risque justifie de manière plus générale la mise en œuvre de mesures techniques et organisationnelles et elle est également intégrée à l'information renforcée qui doit être dispensée à l'individu. Cette approche par les risques, composante du processus de responsabilisation et notamment soutenue au niveau national[1232], semble ainsi être une réponse adaptée aux problématiques posées par les objets connectés et par le *quantified-self*.

619. La difficulté d'appréciation du risque. Pourtant, malgré une liste d'éléments illustrant les conséquences éventuelles de la survenance du risque, le

[1230] Considérant 75 du Règlement (UE) 2016/679.
[1231] Considérant 85 du Règlement (UE) 2016/679.

recours à cette notion par le RGPD comme élément déterminant de la régulation est source d'incertitudes. La méthodologie de calcul du risque proposée au considérant 76, appréciée à l'égard des deux variables qui sont la probabilité et la gravité, pose en effet certains problèmes d'interprétation, notamment quant aux modalités pratiques de calcul d'un tel risque. Dans le cadre du *quantified-self*, comment déterminer qu'il sera fait atteinte à la réputation d'une personne lorsque des données relatives à l'évolution du poids ou au régime alimentaire sont divulguées ? Ces éléments peuvent être appréciés différemment par les personnes concernées par des traitements de données et le RGPD ne mentionne pas le contexte dans lequel s'inscrit le risque éventuel devant faire l'objet d'une appréciation. Enfin, la référence généralisée au « risque élevé », que ce soit pour la nécessité de réaliser une analyse d'impact ou pour l'obligation de notifier une faille de sécurité, mériterait d'être clarifiée. Dans le premier cas, le risque est simplement le préalable à la mise en œuvre d'une analyse des conséquences éventuelles d'un traitement de données à caractère personnel alors que dans le second, celui-ci est déjà susceptible d'être en cours de réalisation.

Le recours au droit souple qui sera dégagé par le Comité européen de la protection des données permettra de compléter ces dispositions. A l'heure actuelle, il est déjà possible de se référer aux lignes directrices du G29 sur la mise en œuvre d'une analyse d'impact pour préciser l'interprétation de la notion. Celui-ci établit une liste de procédés susceptibles d'engendrer un risque élevé au regard des critères dégagés notamment à l'article 35, paragraphe 3 du Règlement[1233]. Le *quantified-self* est inclus à cette liste et ces différents éléments doivent permettre de manière plus générale de rétablir la confiance des utilisateurs envers les services utilisés. Par ailleurs, les risques qu'ils sont susceptibles de faire courir sont identifiés en amont du traitement et des mesures permettant d'en limiter la probabilité et la réalisation sont mises en œuvre.

[1232] Anne-Yvonne Le Dain, Philippe Gosselin, *Rapport d'information sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française*, n° 4544, 22 février 2017, p. 30

[1233] G29, 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, WP 248 rév. 01, 4 avril 2017, p. 9.

2. Un dispositif concurrentiel fondé sur la confiance

620. L'instauration de relations de confiance. La mise en œuvre du RGPD doit répondre au *privacy paradox* déjà identifié. Celui-ci doit en effet permettre l'instauration de mesures visant à établir la confiance des utilisateurs envers les services qu'ils utilisent, confiance qui doit contrebalancer les risques identifiés dans le cadre des applications utilisées par le *quantified-self*[1234]. Le terme de confiance est expressément employé par certains textes[1235] et d'autres puisent dans le même champ lexical, telle que la loi pour une République numérique qui consacre une section entière à la loyauté des plateformes et à l'information des consommateurs. Cette référence croissante à la confiance s'explique notamment par les faits de surveillance attribués à certains Etats et à certaines entreprises du numérique[1236] et elle est également justifiée par le développement d'outils technologiques dont les modalités de fonctionnement peuvent sembler obscures pour les non-initiés. Cette absence d'emprise sur les capacités techniques de traitements de données renforce le risque que les individus ne soient pas en mesure de contrôler totalement les informations divulguées et la façon dont celles-ci sont ensuite réutilisées. Prenant en considération cet élément ainsi que celui relatif à la mondialisation et à la multiplication des transferts internationaux, le RGPD insiste dès lors sur la nécessité de « susciter la confiance qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur »[1237].

Dès 2012, la Commission européenne s'est penchée sur la nécessité de développer un cadre cohérent pour renforcer la confiance dans le marché unique du numérique, au regard du défi posé par les évolutions technologiques aux activités économiques traditionnelles et aux règles administratives qui les gouvernent[1238]. La question de la protection des données à caractère personnel a alors semblé, dans un premier temps, constituer un frein au développement de ce cadre[1239]. Mais ensuite, la

[1234] Conseil National de l'Ordre des médecins, *Livre Blanc sur la santé connecté*, janvier 2015, p. 16.
[1235] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[1236] Anne Debet, « Programme Prism : les citoyens européens sur écoute », *Recueil Dalloz*, 2013, p. 1736.
[1237] Considérant 7 du Règlement (UE) 2016/679.
[1238] Communication de la Commission, *Un cadre cohérent pour renforcer la confiance dans le marché unique numérique du commerce électronique et des services en ligne*, COM (2011) 942 final/2.
[1239] Guido Manfellotto, « La construction du marché unique numérique entre harmonisation et protection des consommateurs », *Revue de l'Union Européenne*, 2017, p. 418.

garantie que les données soient traitées de manière vertueuse est apparue cruciale pour permettre la constitution de ce marché unique et pour renforcer la confiance des utilisateurs envers les services et dispositifs utilisés. La présidente de la CNIL soulignait ainsi que cette « cette « logique de marché ne saurait en aucun cas heurter de front celle de la protection des données personnelles »[1240]. Le renforcement du droit des personnes, désormais harmonisé par le recours à un règlement en lieu et place d'une directive, s'accompagne ainsi de mesures permettant de susciter la confiance par les responsables de traitement. Ceux-ci ont de plus en plus tendance à recourir à des assurances permettant de couvrir le risque cyber[1241] et l'instauration progressive de mesures de protection *ex ante* renforce également la tendance à l'autorégulation, notamment par le développement de modèles économiques fondées sur la conformité à la réglementation.

621. L'avantage concurrentiel. Les risques financiers qui pèsent sur les entreprises les incitent à prendre, en amont, des mesures visant à sécuriser les données. Mais le développement de traitement respectueux des informations nominatives devient également un avantage concurrentiel[1242]. En effet, le principe de conformité prôné par le Règlement général permet l'émergence de nouveaux modèles économiques centrés sur le respect, par les responsables de traitement, des mesures développées par le texte européen. Le respect de recommandations, à l'image du kit publié par l'ANSSI sur la sécurité [1243], contribue à renforcer ce modèle. Ainsi, lorsqu'une entreprise s'engage sur la voie de la responsabilisation et de l'*accountability*, le modèle de traitement des données qui est mis en œuvre permet également d'impacter favorablement la confiance des utilisateurs. Un dispositif connecté ayant fait l'objet de mesures techniques permettant la protection des données par défaut permettra, à l'image d'une application de *quantified-self* sécurisée, de susciter plus d'intérêt de la part des consommateurs. Le recours à des mécanismes protecteurs en tant qu'argument compétitif pourra, par effet

[1240] Isabelle Falque-Pierrotin, « La CNIL face à l'économie de la donnée », *AJCA* 2016, p. 175.
[1241] Jean Cazeneuve, « La cybercriminalité : l'émergence d'un nouveau risque », *AJ pénal*, 2012, p. 268.
[1242] Laurent Heslault, « Transformer le GDPR en avantage concurrentiel en intégrant la protection des données dès la conception des projets », Les Echos, 18 janvier 2017, accessible en ligne à cette adresse : https://www.lesechos.fr/idees-debats/cercle/cercle-165052-transformer-le-gdpr-en-avantage-concurrentiel-en-integrant-la-protection-des-donnees-des-la-conception-des-projets-2058160.php
[1243] Disponible en ligne à cette adresse : https://www.ssi.gouv.fr/administration/reglementation/rgpd-renforcer-la-securite-des-donnees-a-caractere-personnel/

d'entraînement, contribuer à l'instauration d'une culture de la protection des données à caractère personnel directement par les entreprises elle-même.

Le développement de bonnes pratiques à but concurrentiel est propre au droit souple, celui-ci pouvant en effet être produit par n'importe quel acteur, indépendamment de sa nature juridique[1244]. La portée de ce droit spontané peut, de prime abord, sembler limitée. Pourtant, le développement de ce droit souple, dans un contexte concurrentiel, permet à des normes développées au sein d'une entreprise d'être éventuellement reprises et adaptées par d'autres. Une entreprise s'engageant à mettre en œuvre des bonnes pratiques lorsqu'elle traite des données grâce à une application de *quantified-self* (par exemple, l'hébergement systématique des données d'activité sensibles sur des serveurs sécurisés gérés par des hébergeurs agréés) pourrait inciter d'autres entreprises à adopter des pratiques similaires. Cette élaboration de règles de droit souple au sein de l'entreprise contribue ainsi à la régulation des traitements de données à caractère personnel, tout en dotant les entreprises d'instruments relativement souples. La portée de ces règles n'est pas encore comparable à certains documents, tels que ceux proposés par la CNIL. Mais ce recours au droit souple doit permettre, selon son acception classique, de favoriser l'encadrement de domaines émergents[1245] tel que celui des objets connectés et du *quantified-self*.

Le RGPD contribue également à ce mouvement par la mise en œuvre de mécanismes de certification qui permettent d'attester du déploiement de procédures de traitement vertueuses.

B. Les procédures de certification

622. La révolution numérique modifie « profondément le rapport à la norme, qu'il s'agisse de sa substance, de son élaboration ou de son application »[1246]. Ainsi, l'accompagnement de l'innovation implique de « passer d'une logique de

[1244] Conseil d'Etat, *op. cit.*, p. 40.
[1245] Jacky Richard, Laurent Cytermann, « Le droit souple : quelle efficacité, quelle légitimité, quelle normativité ? », *AJDA*, 2013, p. 1884.
[1246] Edouard Geffray, « Droits fondamentaux et innovation : quelle régulation à l'ère numérique ? », *Les nouveaux Cahiers du Conseil constitutionnel*, n°52, juin 2016, p. 7.

réglementation à une logique de régulation, c'est-à-dire à un type d'encadrement et d'accompagnement qui combine la fidélité à des principes fondamentaux et à une règle de droit claire et des nouveaux modes d'intervention du régulateur, fondés sur le droit souple »[1247]. Le Conseil d'Etat, dans son étude annuelle de 2013, préconise une certaine rationalisation du recours au droit souple[1248]. Celle-ci se traduit notamment par une clarification des modalités de recours à un tel droit ainsi que par une meilleure diffusion des prescriptions édictées.

Le RGPD s'inscrit dans ce processus de systématisation et propose, pour assurer la conformité aux règles établis, une large gamme d'outils tels que la certification, les labels ou les marques[1249]. L'article 24 du Règlement prévoit ainsi que l'application de mécanismes de certification approuvés peut servir d'élément permettant de démontrer le respect des obligations incombant au responsable du traitement. Encouragé par les Etats membres, les autorités de contrôle, le comité et la Commission, le recours à ces mécanismes de certification permet de procéder à une évaluation de la conformité **(1)** ; aussi, la mise en œuvre de ces outils est-elle complétée par d'autres dispositifs, en particulier par la normalisation **(2)**.

1. Un processus encouragé

623. Les objectifs. La certification est un mécanisme permettant, de manière générale, de démontrer la conformité au Règlement des opérations réalisées. Celui-ci est identifié par le texte comme pouvant avoir plusieurs utilités précises : identification du risque éventuel et de sa portée[1250], preuve de la protection dès la conception et par défaut[1251], preuve des garanties suffisantes apportées par un sous-traitant[1252] ou encore preuve de la sécurité du traitement[1253]. La mise en place de mécanismes de certification doit « favoriser la transparence et le respect du présent règlement » et permettre aux individus concernés par des traitements de données à

[1247] *Ibid.*
[1248] Il détermine notamment trois critères de recours au droit souple fondé sur un test d'utilité, un test d'effectivité et un test de légitimité.
[1249] Marie-France Mazars, Wafae El Boujemaoui, « Maîtriser le socle du droit de la protection des données pour aborder l'application du Règlement européen (RGPD) », *Rev. trav.*, 2018, p. 298.
[1250] Considérant 77 du Règlement.
[1251] Article 25, 3° du Règlement (UE) 2016/679.
[1252] Article 28, 5°. Du Règlement (UE) 2016/679.

caractère personnel « d'évaluer rapidement le niveau de protection des données offerts par les produits et services en question »[1254]. La portée de ce processus de certification, limitée sous l'empire de la loi Informatique et Libertés modifiée de 1978[1255], est désormais généralisée.

Permettant non seulement de s'inscrire dans le processus de renforcement de l'information délivrée aux individus, ce recours généralisé à la certification doit permettre aux individus une meilleure visibilité sur les produits et services utilisés, compte tenu du nombre croissant de ces services. Research 2 guidance, firme de *consulting* spécialisée dans le marché des applis mobiles, estime qu'il y'a 325 000 applications relatives au *quantified-self*[1256]. La certification, complétée par l'instauration de labels et de marques démontrant le respect des règles européennes, permet d'ajouter à la réglementation prescriptive une « régulation plus partenariale, fondée sur des instruments juridiques personnalisés » [1257] et fait l'objet d'un encadrement particulier par le Règlement.

624. Les modalités. Selon l'article 42, 3° du RGPD, la certification est « volontaire et accessible via un processus transparent » et celle-ci doit faire l'objet d'une approbation par des organismes de certification, par l'autorité de contrôle compétente ou par le Comité européen. Cette relation institutionnelle tripartite vise à garantir l'efficacité de la certification. En effet, les organismes de certification privés doivent remplir certains critères d'indépendance et d'expertise. Or, ces critères sont présumés lorsque le Comité ou des autorités de contrôle ont pour mission d'élaborer ou d'approuver des référentiels. Ce mécanisme du recours à la certification n'est en soi pas novateur puisque la CNIL délivrait déjà des labels, présentés comme des indicateurs de confiance offrant des avantages concurrentiels[1258]. L'orientation européenne permet d'uniformiser le recours à ce type d'outils en mettant à

[1253] Article 32, 3° du Règlement (UE) 2016/679.
[1254] Considérant 100 du Règlement (UE) 2016/679.
[1255] L'article 11 de cette loi, relatif aux missions de la CNIL, indique que celle-ci peut « certifier ou homologuer et publier des référentiels ou des méthodologies générales aux fins de certification de la conformité à la présente loi de processus d'anonymisation des données à caractère personnel ».
[1256] R2G, *mHealth App Economics*, 2017, 26 p.
[1257] Isabelle Falque-Pierrotin, « Le droit souple vu de la CNIL : un droit relais nécessaire à la crédibilité de la régulation des données personnelles », *in* Rapport du Conseil d'État, *Le droit souple*, *op. cit*., p. 241.
[1258] https://www.cnil.fr/fr/les-labels-cnil

contribution chacune des autorités de contrôle nationale. Le procédé mis en œuvre par le RGPD peut sembler complexe, mais le contrôle qui est opéré par les autorités ou par le Comité européen est apparu nécessaire. Le risque est en effet que cet instrument de conformité, mal appliqué, perde de son utilité première et se transforme en simple formalité préalable, même si la certification ne diminue pas, selon l'article 42, 4°, la responsabilité du responsable de traitement ou du sous-traitant.

Le RGPD permet également la mise en œuvre de labels, sur la base de critères approuvés et publiés par l'autorité de contrôle compétente et par le Comité européen. Le texte ne précise pas exactement quels sont ces critères et un responsable de traitement ou un sous-traitant peut également s'adresser à une entité privée pour la délivrance d'un label. Le Parlement européen souhaitait que ce rôle soit uniquement dévolu aux autorités nationales de contrôle en matière de protection des données personnelles mais la Commission européenne et le Conseil ont également souhaité accréditer les auditeurs privés[1259]. Le compromis adopté, entre contrôle par des entités publiques et privées, renforce la co-régulation qui existe en matière de protection des données à caractère personnel et l'association d'entités publiques et privées aux fins de la certification et de la délivrance de labels permet le développement d'une régulation pragmatique. Celle-ci est dès lors fondée sur un dialogue entre acteurs aux intérêts divergents, entre liberté de traiter des données, à des fins économiques, et protection des libertés des individus. Le procédé mis en place doit alors contribuer à rétablir la confiance envers les opérateurs du numérique[1260], en raison notamment du contrôle des organismes privés de certification mis en œuvre par l'article 43 du Règlement.

625. Portée et limites. Le résultat final de la certification peut prendre plusieurs formes, parmi lesquels le label ou la marque[1261] mais le RGPD ne fait pas de

[1259] Claire Levallois-Barth, *op. cit.*, p. 142.
[1260] Il est possible, en l'absence de définition législative de la notion, de faire référence à celle donné dans le Vocabulaire juridique du Doyen Gérard Cornu qui indique que celle-ci est la « croyance en la bonne foi, loyauté, sincérité et fidélité d'autrui (tiers, contractant) ou en ses capacités, compétences et qualifications professionnelles », Gérard Cornu, *Vocabulaire juridique*, Paris, PUF, 11e édition, 2016.
[1261] Le « label européen de protection des données » mentionné par l'article 42, 5° est ainsi le résultat d'une certification commune.

distinction et soumet en théorie ces trois instruments à approbation[1262]. Outils d'un droit qui « invite plus qu'il ne contraint, qui propose plus qu'il n'impose, qu'il dirige plus qu'il ne force »[1263], ils sont également susceptibles d'engendrer une certaine contrainte pour les responsables de traitement. Les sanctions ne sont pas d'ordre pécuniaire mais le retrait de certification peut être perçu comme « une sanction morale préjudiciable à l'image de l'entreprise »[1264] dans un contexte ou le respect de la protection des données doit être perçu comme un avantage concurrentiel. La question du coût de cette certification est cependant susceptible d'en limiter la portée. Les grandes entreprises du numérique pourront facilement y recourir mais il en va différemment des firmes aux capacités financières réduites, micro, petites et moyennes entreprises, qui préféreront se tourner vers les codes de conduite ou vers des normes volontaires.

2. Un processus complété

626. L'article 1er du décret n° 2009-697 du 16 juin 2009 relatif à la normalisation définit celle-ci comme « une activité d'intérêt général qui a pour objet de fournir des documents de référence élaborés de manière consensuelle par toutes les parties intéressées, portant sur des règles, des caractéristiques, des recommandations ou des exemples de bonnes pratiques, relatives à des produits, à des services, à des méthodes, à des processus ou à des organisations ». La normalisation se caractérise ainsi, pour les entreprises, par une application volontaire de normes dont les modalités d'élaboration impliquent la recherche du consensus. Une triple évolution a permis son affirmation progressive : l'insertion dans un cadre régulé par les pouvoirs publics, la participation au développement des échanges internationaux et la diversification des sujets couverts[1265]. A ce titre, la normalisation s'inscrit dans un cadre « prévu par le droit dur assurant le contrôle des pouvoirs publics »[1266], bien que l'élaboration des normes soit assurée par les parties intéressées. L'Association

[1262] L'article 42 du RGPD indique que « les mécanismes de certification, les labels ou les marques en matière de protection des données approuvés en vertu du paragraphe 5 du présent article », bien que le paragraphe 5 ne fasse par la suite uniquement référence à la certification.
[1263] Mustapha Mekki, Propos introductifs sur le droit souple, *in* Association Henri Capitant, *Le droit souple*, Dalloz, Coll. « Thèmes et Commentaires », 2009, p. 11.
[1264] Claire Levallois-Barth, *op. cit.*, p. 33.
[1265] Conseil d'Etat, *op. cit.*, p. 41.

française de normalisation (AFNOR) a été créée en 1926 et une loi du 24 mai 1941 a donné compétence au pouvoir réglementaire pour fixer le statut de la normalisation par décret. Le Conseil d'Etat considère que l'AFNOR exerce une mission de service public[1267] et que l'homologation d'une norme relève de la mise en œuvre de prérogatives de puissance publique pouvant être contestée devant le juge administratif[1268]. Pourtant, « la norme homologuée reste cependant d'application facultative, et relève ainsi du droit souple »[1269].

627. Des normes volontaires. La particularité de ces normes dites « volontaires » est de fournir un « cadre de référence qui vise à fournir des lignes directrices, des prescriptions techniques ou qualitatives pour des produits, services ou pratiques au service de l'intérêt général »[1270]. Les normes qui sont créées ont la particularité d'être le fruit d'une « co-production consensuelle entre les professionnels et les utilisateurs qui se sont engagés dans son élaboration »[1271]. Ces normes volontaires permettent de compléter les dispositions législatives et réglementaires en apportant des précisions quant aux pratiques à mettre en œuvre pour s'y conformer. Le mécanisme ainsi développé repose sur une approche ascendante ou *bottom-up*, en opposition à une approche descendante ou *top-down*. Des dispositions législatives à portée générale sont en effet précisées par les responsables de traitement directement chargés de les appliquer et ces derniers deviennent, par conséquent, créateurs de normes.

628. Des normes adaptées au *quantified-self*. Le cadre régulateur offert par la normalisation semble particulièrement adapté au déploiement des objets connectés. Au sein de l'AFNOR, une commission de normalisation sur l'IOT a d'ailleurs été créée pour mettre en place un cadre d'interopérabilité adapté[1272]. Par ailleurs, l'AFNOR a publié un guide pratique sur les normes volontaires en matière de

---

[1266] *Ibid*.
[1267] CE, 17 février 1992, *Société Textron*, n° 73230, Rec. p. 66.
[1268] CE, 14 octobre 1991, *Section régionale « Normandie Mer du Nord » du comité interprofessionnel de conchyliculture et Quetier*, n° 90260, Rec. p. 777.
[1269] Conseil d'Etat, *op. cit*., p. 42.
[1270] AFNOR, *Guide Protection des Données personnelles : l'apport des normes volontaires*, janvier 2017, p. 19.
[1271] *Ibid.*
[1272] https://normalisation.afnor.org/thematiques/numerique/

protection des données afin d'expliquer l'intérêt des normes ISO pour la sécurité de l'information et pour la protection de la vie privée. L'approche préconisée par l'AFNOR repose sur la gestion des risques et elle doit permettre de protéger à la fois l'organisme (des risques relatifs à la cybersécurité notamment) et les individus (des risques quant à leurs libertés individuelles)[1273]. Plusieurs normes volontaires ISO, « rédigées par des professionnels pour des professionnels »[1274], ont ainsi été publiées pour promouvoir les bonnes pratiques de protection de la vie privée spécifiques au *cloud computing*, [1275], aux techniques de cryptographie[1276] ou aux techniques d'anonymisation[1277].

Les normes ainsi créées ont la double particularité d'apporter des précisions utiles d'un point de vue technique - on parle d'ailleurs de « normes techniques » - mais aussi d'avoir un champ d'application élargi dans la mesure ou le niveau mondial[1278] est le niveau privilégié de leur élaboration[1279]. Le recours à la normalisation et à des normes volontaires créées directement par des entités privées en charge du traitement de données à caractère personnel est susceptible de pallier les insuffisances actuelles du cadre juridique et à son éventuelle fragmentation, en l'absence d'un cadre international commun de protection. Le recours à la normalisation technique est dès lors susceptible de contribuer à l'instauration d'un cadre international de bonnes pratiques, cadre qui doit d'appliquer aux développeurs d'objets connectés et d'applications utilisées dans le domaine du *quantified-self*.

La mise en place *ex ante* de bonnes pratiques contribuent ainsi au développement d'un cadre commun et global de protection. Certaines problématiques rencontrées dans le cadre du *quantified-self*, relatives notamment à la classification des données traitées et au régime juridique applicable, pourraient ainsi s'effacer pour laisser place à un cadre protecteur spécifiquement adapté aux spécificités de l'automesure. Procéder ainsi permettrait ainsi une meilleure protection des droits des

[1273] AFNOR, *op. cit.*, p. 5.
[1274] *Ibid*, p. 14.
[1275] Code of practice for protection of personally identifiable information (PII) in public clouds (ISO/IEC27018).
[1276] Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191).
[1277] Privacy enhancing data de-identification techniques (ISO/IEC 20889).
[1278] *International Standard Organisation* (ISO), créée en 1947.
[1279] Conseil d'Etat, *op. cit.*, p. 42.

individus et limiterait donc le contentieux. Ce dernier fait d'ailleurs l'objet d'un nouveau partage, au regard du système particulier mis en œuvre à l'origine par la loi Informatique et Libertés et repris par le RGPD.

SECTION II. LE NOUVEAU PARTAGE DU CONTENTIEUX

629. La création par la loi Informatique et Libertés de 1978 d'une autorité administrative chargée de la protection des données à caractère personnel a entraîné la mise en œuvre d'un système répressif original, entre sanctions administratives et sanctions judiciaires de nature pénale. La CNIL ne disposait à l'origine d'aucuns pouvoirs répressifs mais l'évolution des modalités de collecte et de traitement des données a justifié, dès 2004, que celle-ci soit dotée de moyens d'action permettant de réprimer les atteintes à la réglementation. A ce titre, le développement du numérique et la multiplication des traitements de données ont justifié la mise en œuvre d'un système particulier de sanction. En effet, en dehors des cas de piratages massifs, tels que celui ayant touché l'application *My Fitness Pal*, les infractions à la législation sont rendues particulièrement complexes à identifier par la miniaturisation des dispositifs employés et par le nombre de traitement réalisés.

La pertinence du cadre juridique précédemment établi et récemment rénové nécessite, pour être appréciée, que les individus soient dotés de voies de recours leur permettant de faire efficacement valoir leurs droits. La particularité des infractions a justifié que l'autorité en charge de valider la mise en œuvre des traitements soit également en charge de sanctionner les atteintes à la réglementation. La protection juridictionnelle a été redistribuée **(Paragraphe 1)**, mais aussi externalisée, pour répondre au caractère transfrontalier des traitements mis en œuvre **(Paragraphe 2)**.

§1. Une protection juridictionnelle redistribuée

630. Les pouvoirs d'intervention de la CNIL étaient à l'origine limités. La loi du 6 janvier 1978 lui permettait de procéder à des vérifications sur place mais ce contrôle était peu utilisé, la CNIL n'ayant effectué qu'un peu plus de 300 missions de

vérification en vingt-cinq ans[1280]. En dehors de ces vérifications, la CNIL pouvait uniquement délivrer des avertissements aux responsables de traitement ou les dénoncer au parquet lorsqu'elle constatait un manquement à la loi. En résultait une jurisprudence clairsemée **(1)** qui a justifié, par suite de la transposition de la directive 95/46/CE par la loi du 6 août 2004, que les pouvoirs de sanctions administratives de la CNIL soient renforcés et qu'un rôle croissant lui soit progressivement accordé **(2)**.

A. Les limites de l'approche juridictionnelle

631. La mise en œuvre de la loi Informatique et Libertés reposait, lors de son adoption en 1978, sur le recours au juge judiciaire pour trancher les éventuels litiges et engager la responsabilité du responsable de traitement ou des tiers. Le nombre de décisions ayant été rendues sur ce fondement montre pourtant les limites inhérentes à ce système. Cette voie de recours étant peu utilisée et n'apportant pas de réponse *a posteriori* adaptée, une autre approche, fondée sur le prononcé de sanctions administratives et faisant de la CNIL le gardien des libertés individuelles, lui a été préférée. Interlocutrice privilégiée des personnes concernées par des traitements de données, la CNIL s'est vu attribuer des pouvoirs de sanction, confirmant ainsi le choix d'un traitement administratif des litiges. Ces éléments ont contribué au retrait du juge judiciaire **(1)**, actant l'inadéquation de la réponse pénale initialement proposée **(2)**.

1. Un juge judiciaire en retrait

632. Le rapport Braibant de 1998, rédigé à la suite de l'adoption de la directive 95/46/CE, insistait sur la répartition naturelle du contentieux susceptible de naître d'un traitement de données à caractère personnel. L'article 22 de la directive rappelait que la voie du recours juridictionnel restait ouverte « sans préjudice du recours administratif qui peut être organisé » et le rapport prônait une répartition selon les principes généraux de notre droit du contentieux : devant les tribunaux de l'ordre judiciaire lorsque le responsable de traitement était une personne privée et devant

[1280] Florence Fourets, « La protection des données, ou le symbole d'une démocratie nouvelle. Le contrôle de la CNIL », *Informations sociales*, vol. 126, no. 6, 2005, pp. 94-103.

ceux de l'ordre administratif lorsqu'il s'agissait d'une personne publique, étant entendu que les décisions de l'autorité de contrôle étaient uniquement susceptibles de recours devant le juge administratif[1281]. Le juge judiciaire est cependant resté dans une position « excessivement en retrait dans la mise en œuvre de la loi de 1978 »[1282].

Il existe aujourd'hui peu de jurisprudence sur la condamnation d'un responsable de traitement pour non-respect des formalités préalables. Il est possible de relever des exemples de condamnations basées sur plusieurs infractions, dont le non-respect des formalités, mais ceux-ci ne permettent pas de « souligner pleinement l'importance du respect des formalités préalables à un traitement de données personnelles », les cas recensés ayant ainsi « un caractère anecdotique, voire dérisoire » [1283]. Les décisions relatives au détournement de finalité des traitements[1284] ou à la divulgation de données personnelles sans autorisation[1285] sont également rares. Cette absence de positionnement de la part des juridictions est renforcée, à partir de 2004, par les pouvoirs de sanction qui sont attribués à la CNIL. Alors que celle-ci était précédemment uniquement investie d'une mission de collaboration avec le pouvoir judiciaire[1286], la réforme de la loi de 1978 en 2004 a contribué au changement de son statut.

633. Conformément à la position déjà adoptée dans son rapport public pour l'année 2001 sur les autorités administratives indépendantes[1287], le Conseil d'Etat a considéré dans une décision du 19 février 2008 que la CNIL est un organisme administratif qui « eu égard à sa nature, à sa composition et à ses attributions, peut être qualifié de tribunal au sens de l'article 6-1 de la Convention européenne de

[1281] Guy Braibant, *Données personnelles et société de l'information*, Rapport au premier ministre, Documentation Française, 1998, p. 119.
[1282] Céline Bloud-Rey, « Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ? », *Recueil Dalloz*, 2013, p. 2795.
[1283] Fabrice Mattatia, « CNIL et tribunaux : concurrence ou complémentarité dans la répression des infractions à la loi informatique et libertés ? », *RSC*, 2009, p. 317.
[1284] CA Aix-en-Provence, 5e chambre correctionnelle, 21 sept. 2005, LexisNexis SA, JurisData 2005-291612.
[1285] CA Paris, chambre correctionnelle 9 section B, 17 sept. 2004, LexisNexis SA, JurisData 2004-255097.
[1286] L'article 11, 2°, e) dispose que la CNIL « informe sans délai le procureur de la République, conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance, et peut présenter des observations dans les procédures pénales ».
[1287] « 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) », Conseil d'Etat, Rapport Public 2001, Jurisprudence et avis de 2000, Les autorités administratives indépendantes, La Documentation Française, Etudes & Documents n°52, p. 360.

sauvegarde des droits de l'homme et des libertés fondamentales »[1288]. Cette qualification est de nature à entraîner certaines conséquences procédurales pour la CNIL[1289]. Le Conseil constitutionnel a en effet admis qu'un cumul de sanctions était possible, à la condition que le montant global ne puisse dépasser le montant le plus élevé de l'une des sanctions encourues. Ce cumul de sanctions était expressément prévu par la loi Informatique et Libertés qui indiquait en son article 47 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 la sanction pécuniaire s'impute sur l'amende qu'il prononce ». La loi adoptée le 14 mai 2018 reprend cette distinction et confirme qu'une double saisine est possible, bien qu'en pratique, les sanctions prononcées par la CNIL soient plus dissuasives que celles prononcées par le juge.

Deux raisons ont pu être invoquées pour expliquer cette différence[1290]. D'abord, un responsable de traitement ne respectant pas les dispositions de la loi Informatique et Libertés pourra éviter une sanction en se conformant directement à la mise en demeure prononcée par la CNIL. A titre d'exemple, une mise en demeure concernant les objets connectés a été prononcée par la CNIL en décembre 2017, fondée sur un défaut de sécurité de l'objet et sur un défaut d'information des utilisateurs des jouets[1291]. Cette mise en demeure, qui n'est pas une sanction, constitue la première étape du dispositif répressif. Lorsque le responsable de traitement se conforme à la mise en demeure, le président de la CNIL peut prononcer la clôture de la procédure. Ainsi, la sanction ne sera prononcée que dans le cas où le délit se poursuit, malgré l'avertissement et cette « persévérance dans l'infraction peut alors expliquer la lourdeur de la sanction »[1292].

Ensuite, la seconde raison tiendrait à l'inadéquation de la réponse pénale apportée aux violations de la réglementation protectrice des données, bien que le RGPD reprenne cette distinction entre sanctions administratives et sanctions pénales.

[1288] Conseil d'État, Juge des référés, 19/02/2008, 311974, Inédit au recueil Lebon.
[1289] Romain Perray, « Quel avenir pour le pouvoir de sanction de la CNIL ? », *Lamy Droit de l'Immatériel*, janv. 2008, n°34, p. 82.
[1290] Fabrice Mattatia, article précité, p. 486.
[1291] CNIL, Décision n° MED-2017-073 du 20 novembre 2017 mettant en demeure la société GENESIS INDUSTRIES LIMITED.
[1292] *Ibid*.

2. L'inadéquation de la réponse pénale

634. La protection limitée. La loi Informatique et Libertés de 1978 a institué un système répressif reposant sur le recours au juge pénal. Les articles 226-16 et suivants du code pénal prévoient une série d'infractions relatives notamment au défaut de formalités préalables[1293], au traitement réalisé par un moyen frauduleux, déloyal et illicite[1294] ou encore au traitement opéré malgré l'opposition de la personne concernée[1295]. La jurisprudence n'est pas abondante mais la portée des dispositions pénales ne doit pas être négligée lorsque celles-ci sont effectivement mises en oeuvre[1296]. Elles sont notamment révélatrices du recours par le juge pénal à un ensemble élargi et varié d'incriminations, telles que la non-déclaration du traitement, la collecte de données par un moyen frauduleux ou le défaut d'information des personnes concernées[1297]. En l'absence de pouvoirs de sanctions à disposition de la CNIL avant la transposition en 2004 de la directive 95/46/CE, ces solutions rendues sur le plan pénal ont permis de passer outre l'inertie de la CNIL qui n'a pas toujours procédé effectivement à la dénonciation au parquet des infractions dont elle a eu connaissance[1298].

La jurisprudence pénale a, à certains égards, permis d'instaurer une protection des individus concernés par des traitements de données. Pourtant, ce type de recours est rapidement apparu limité en pratique. D'un point de vue conceptuel d'abord, le droit pénal ne semble guère le bienvenu au sein du cyberespace en ce que les « limites à la liberté et la répression qu'il évoque » semble en profonde contradiction avec « l'idéal de liberté totale des tenants d'un internet déconnecté de tout ordre juridique »[1299]. Une autre limite serait ensuite relative à la définition restrictive de la notion de traitement automatisé parfois retenue en jurisprudence[1300], à l'image de la Chambre criminelle de la Cour de cassation[1301]. Cette solution est antérieure aux

[1293] Article 226-16 du Code pénal.
[1294] Article 226-18 du Code pénal.
[1295] Article 226-18-1 du Code pénal.
[1296] Jacques 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.
[1297] Trib. corr. Paris, 17e ch., 16 déc. 1994, affaire « Risqu'assur ».
[1298] Jean-Paul Carminati, « Les non-dénonciations de la CNIL au parquet. Une pratique contra legem aux effets pervers », *Expertises*, février / mars 1995, p. 67 et 106.
[1299] Agathe Lepage, « Droit pénal et internet : la part de la tradition, l'oeuvre de l'innovation », *AJ pénal*, 2005, p. 217.
[1300] Jacques Francillon, article précité, p. 676.
[1301] Crim. 6 juill. 1994.

développements technologiques relatifs aux moteurs de recherche, aux réseaux sociaux ou aux objets connectés. Mais, l'absence de parquet ou de magistrats spécialisés dans le domaine du numérique pourrait, de manière générale, limiter la portée des réponses coercitives qui seraient apportées aux traitements réalisés en contrariété avec la réglementation. Au regard des différentes évolutions technologiques auxquelles la matière est soumise, l'approche administrative reposant sur une autorité spécialisée semble plus à même d'assurer la protection des droits des individus.

635. La difficulté d'appréciation des atteintes. Autre élément révélateur de l'inadéquation de la réponse pénale aux cas d'infractions à la réglementation protectrice des données, le fait que « « pour le juge pénal, les infractions à la loi informatique et libertés sont bénignes par rapport à la criminalité traditionnelle dont il a à traiter quotidiennement »[1302]. En effet, ces infractions ont pour particularité de ne pas présenter « d'atteinte physique aux personnes ni aux biens » et les préjudices sont « sauf dans les cas d'escroquerie suite à un *phishing*, difficiles à chiffrer, voire virtuels » [1303]. Ces éléments peuvent sans doute justifier la prudence du magistrat et sa retenue dans la répression, étant donné le faible montant des amendes prononcées et le cantonnement des peines de prison à des peines avec sursis. Si les sanctions prononcées par les tribunaux et par la CNIL sont parfois identiques lorsque les atteintes sont similaires[1304], la CNIL se montre généralement plus sévère[1305].

La nature des atteintes permises par les dispositifs de *quantified-self* corrobore ce constat : l'atteinte à l'intimité – la transmission à des tiers de données relatives au poids de l'individu par exemple – sera aisément démontrable lorsqu'un traitement est réalisé en contrariété avec la réglementation. Mais comment chiffrer le préjudice résultant d'une atteinte à l'intimité ? Il est certes possible de chiffrer la valeur qu'une

[1302] Fabrice Mattatia, article précité, p. 486.
[1303] *Ibid.*
[1304] Délibération n° 2007-352 de la CNIL du 22 novembre 2007 et CA Toulouse, 3e chambre correctionnelle, 12 janv. 2005, LexisNexis SA, JurisData 2005-272643.
[1305] Anne Debet, Jean Massot, Nathalie Metallinos, *op. cit.*, p. 851.

donnée à caractère personnel représente pour une entreprise[1306] mais il est plus difficile d'apprécier les conséquences pécuniaires d'une telle atteinte pour l'individu.

Ces différents éléments, tout en révélant les limites relatives à l'approche pénale de la matière[1307], ont contribué au renforcement progressif des pouvoirs de la CNIL.

B. Le rôle croissant de la CNIL

636. La CNIL, première autorité administrative indépendante à avoir été créée en France, a dû répondre aux défis que l'évolution des technologies a posé aux libertés. Anticipant l'exigence de la directive 95/46/CE relative à l'instauration d'autorités de contrôle indépendante, sa création a notamment eu pour but l'observation et la régulation d'un secteur reposant sur des technologies en pleine émergence et aux possibilités techniques encore inconnues à l'époque. L'indépendance de la CNIL, garantie de son autorité, s'exerce ainsi à l'égard non seulement du gouvernement et du Parlement, mais également à l'égard des personnes contrôlées et donc des responsables de traitement. Face aux limites d'une répression pénale peu adaptée à la matière, doter la CNIL de pouvoirs de sanction renforcés a semblé permettre une meilleure protection des individus, au regard notamment de son expertise technique et de sa connaissance des enjeux. Ce pouvoir de sanction était originellement limité voire symbolique[1308], mais la révision de la LIL par la transposition de la directive 95/46/CE lui a conféré d'importants pouvoirs en ce domaine **(1)**, supposant de repenser ses autres missions **(2)**.

1. Un pouvoir de sanction renforcé

637. La CNIL, selon la version initiale de la loi de 1978 et son article 21, 4°, ne pouvait prononcer qu'un avertissement. Tout au plus pouvait-elle dénoncer au parquet les infractions dont elle avait connaissance, procédure dont elle a fait un

[1306] Boston Consulting Group, *The value of our digital identity*, November 2012, p. 53.
[1307] Agathe 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 », *Droit pénal*, mars 2005, n° 3, étude 5.
[1308] Anne Debet, Jean Massot, Nathalie Metallinos, *op. cit.*, p. 824.

usage limité. Le Conseil d'Etat réfutait au départ sa qualification de juridiction, celle-ci n'étant alors pas considérée comme un tribunal au sens de l'article 6-1 de la Convention européenne des droits de l'homme et des libertés fondamentales[1309]. La loi du 6 août 2004 de transposition de la directive de 1995 a doté la CNIL du pouvoir de prononcer des sanctions, dont certaines relèvent d'une commission restreinte afin d'éviter le cumul des phases de poursuite, d'instruction et de jugement entre les mains d'une même personne[1310]. Les sanctions proprement dites peuvent faire l'objet d'un recours de pleine juridiction devant le Conseil d'Etat et la formation restreinte de la CNIL, également appelée « formation contentieuse », se penche tout particulièrement sur les affaires issues de plaintes ou de contrôles afin de décider si celles-ci sont passibles d'une sanction. Ce pouvoir de sanction de la CNIL a été profondément modifié en 2011 par la loi sur le Défenseur des droits afin de prendre en compte les exigences de la CEDH relatives au droit à un procès équitable[1311].

La CNIL dispose de différents types de sanctions que sa formation restreinte peut mettre en œuvre et prononcer à l'égard du responsable de traitement lorsque des manquements à la loi sont constatés et portés à sa connaissance. La mise en demeure constitue le préalable à la mise en œuvre de ces sanctions et celle-ci doit permettre au responsable de traitement de régulariser sa situation. Si celui-ci ne se conforme pas à la mise en demeure, la formation restreinte peut prononcer un avertissement, une sanction pécuniaire ou encore une injonction de cesser le traitement. D'autres mesures, telles que l'interruption de la mise en œuvre du traitement, l'avertissement ou le verrouillage des données pendant un certain délai, peuvent être prononcées, notamment en cas d'urgence et d'atteinte aux droits et libertés. Avant 2004 et en comparaison à d'autres autorités telles que le Conseil de la concurrence, le Conseil supérieur de l'audiovisuel ou l'Autorité des marchés financiers, la CNIL ne disposait pas réellement d'un pouvoir coercitif. L'exercice de ce pouvoir de sanction, perçu

[1309] CE, 3 décembre 1999, n° 197060 et 197061, publié au recueil Lebon.
[1310] Décret n° 2011-2023 du 29 décembre 2011 relatif aux pouvoirs de contrôle et de sanction de la Commission nationale de l'informatique et des libertés.
[1311] Loi n° 2011-333 du 29 mars 2011.

comme une révolution, a entraîné un changement culturel profond au sein de la CNIL[1312].

638. La plupart des régulateurs considèrent que leur pouvoir de sanction est un instrument indispensable à l'exercice de leur autorité. Si la CNIL n'est pas un régulateur au sens strict du terme – elle ne répartit pas une ressource ou ne surveille pas un marché – elle veille néanmoins à l'application de la loi tout en donnant un certain nombre d'orientations quant aux évolutions, notamment technologiques, qui sont constatées[1313]. A ce titre, au vu du développement des objets connectés et du *quantified-self*, le renforcement des pouvoirs de la CNIL ne peut être que bénéfique pour les individus concernés par des traitements de données à caractère personnel. De plus, la CNIL a développé à plusieurs égards des liens privilégiés avec le Conseil d'Etat. D'abord par la voie du recours de pleine juridiction qui est offerte à ses décisions et ensuite par sa composition, puisque la CNIL accueille deux conseillers d'Etat. Ce lien contribue ainsi à la prise en compte des problématiques du numérique par la plus haute juridiction de l'ordre administratif, à l'image de son étude annuelle pour l'année 2014 portant sur le numérique et les droits fondamentaux.

639. La loi pour une République, anticipant la rénovation du cadre juridique apportée par le Règlement général européen, a renforcé le pouvoir de sanction de l'autorité administrative indépendante. Le plafond maximal de ses sanctions passe de 150 000 à 3 millions d'euros, alors que la formation restreinte de la CNIL peut désormais ordonner aux organismes sanctionnés d'informer individuellement chacune des personnes concernées de cette sanction. Surtout, le mécanisme de la mise en demeure des organismes est dans certains cas supprimé. La CNIL peut en effet prononcer directement des sanctions financières, sans mise en demeure, lorsque le manquement constaté n'est pas susceptible de faire l'objet d'une mise en conformité. Désormais, le RGPD prévoit que les amendes administratives pourront s'élever, selon les catégories d'infractions, de 10 à 20 millions d'euros, ou, dans le cas d'une entreprise, de 2% jusqu'à 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu. Ainsi, le rôle de la CNIL doit prendre « une autre dimension »

[1312] *Ibid.*

avec l'entrée en application du Règlement[1314]. Or, celle-ci a développé de nombreuses mesures extra-judiciaires contribuant à la bonne application de la règlementation, parallèlement à son activité répressive.

2. Des mesures extra-judiciaires repensées

640. Le droit souple. Bien que la CNIL ait été progressivement dotée de pouvoirs de sanction renforcés, celle-ci n'a pas pour autant délaissé ses missions traditionnelles de conseil et d'information. Ainsi la loi Informatique et Libertés indique dans son article 8 que la CNIL « informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations ». Cette information ne concernait à l'origine que les personnes concernées par des traitements de données à caractère personnel mais un amendement a fait ajouter en 2004 la mention de « tous les responsables de traitements », bien que la CNIL n'eût pas attendu cet ajout pour diffuser différents guides d'information les concernant directement[1315]. Cette mise en œuvre d'un droit souple d'origine institutionnelle permet à la CNIL de proposer une interprétation des règles de droit établies au regard des évolutions technologiques constatées. Bien que des recommandations soient publiées par la CNIL, outrepassant parfois la limite du droit souple en établissant une obligation juridique donnant naissance à un contentieux[1316], celle-ci établit aussi des guides pratiques à caractère purement informatif. Différents outils de communication, s'intéressant particulièrement aux technologies innovantes tels que les objets connectés et le *quantified-self*, ont ainsi été publiés.

641. La prospective. La CNIL, consciente de la rapidité des évolutions technologiques développées dans le cadre du numérique, a développé une activité d'études, d'innovation et de prospectives. Celle-ci vise spécifiquement à remplir deux

---

[1313] Olivia Dufour, « L'exercice du pouvoir de sanction est une révolution culturelle pour la CNIL », *Les Petites Affiches*, n° 195, 29 septembre 2004, p. 3.
[1314] Marie-France Mazars, « La CNIL à l'ère du RGPD : la protection des données personnelles renforcée », *Les Cahiers Sociaux*, n° 306, 1er avril 2018, p. 224.
[1315] Anne Debet, Jean Massot, Nathalie Metallinos, *op. cit.*, p. 801.
[1316] Voir par exemple : CE, 30 octobre 2001, n° 204909, publié au recueil *Lebon* et par lequel le Conseil d'Etat a annulé les dispositions de la délibération n° 98-101 de la CNIL du 22 décembre 1998 en ce qu'elle outrepassait la limite de la simple interprétation.

objectifs, à savoir « détecter en amont de nouveaux usages et tendances émergentes » et « explorer des sujets prospectifs touchant aux libertés individuelles et publiques, aux données personnelles et à la vie privée dans l'univers numérique »[1317]. Reposant notamment sur un comité de la prospective composé d'experts issues de différentes institutions (journalistes, universitaires ou encore entrepreneurs), celui-ci est présidé par la présidente de la CNIL et « contribue aux débats sur l'éthique du numérique et constitue un espace d'échanges et de réflexion, ouvert et libre, sur la culture des données »[1318]. La mise en œuvre d'une activité dédiée à l'innovation et à la prospective permet d'anticiper les enjeux juridiques issus du développement de technologies novatrices. Le mécanisme de travail et de réflexion adopté contribue, par sa souplesse, à proposer un certain nombre de travaux aux formes variées. Ceux-ci, en l'absence de dispositions visant à orienter les comportements, ne répondent pas directement aux critères traditionnels du droit souple. Mais ils permettent d'identifier les problématiques en développement et d'anticiper l'éventuelle mise en oeuvre de mesures de droit souple ou d'interpeller le gouvernement ou le parlement sur certaines questions.

Parmi les publications axées sur l'aspect innovation et la prospective, la CNIL a développé un cahier spécialisé ainsi qu'une lettre d'information. Ces médias ont tous deux eu vocation à traiter du développement des objets connectés et du *quantified-self*. La lettre Innovation et Prospective publiée en 2013 a eu l'occasion de faire un premier état des lieux sur le sujet, de montrer l'ambivalence des données collectées dans ce cadre et de poser la question de la régulation à appliquer[1319]. Un an plus tard, le Cahier Innovation et Prospective dédié au corps en tant que nouvel objet connecté analysait l'utilisation des dispositifs utilisés pour la pratique de l'automesure et soulevait des axes de régulation à envisager. Il procédait notamment à une analyse comparative des régulations, mentionnant par exemple la régulation sectorielle en vigueur aux Etats-Unis, procédant à une qualification des applications de *quantified-self* en fonction de leur finalité médicale[1320]. Ces deux publications

[1317] Voir notamment : https://www.cnil.fr/fr/innovation-et-prospective-a-la-CNIL
[1318] https://www.cnil.fr/fr/les-membres-du-comite-de-la-prospective
[1319] CNIL, « Le quantified self : nouvelle forme de partage des données personnelles, nouveaux enjeux ? », *Lettre Innovation & Prospective de la CNIL*, n° 5, juillet 2013.
[1320] CNIL, *Le Corps, nouvel objet connecté, du quantified self à la m-santé : les nouveaux territoires de la mise en données du monde*, Cahiers Innovation & Prospective, n° 2, mai 2014, p. 47.

étaient spécifiquement dédiées à l'automesure connecté mais d'autres lettres ou cahiers ont également pu contribuer à la réflexion, qu'il s'agisse du cahier relatif à la vie privée à l'horizon 2020 et présentant les évolutions sociologiques et juridiques de la notion[1321], ou de la lettre relative aux applications pour *smartphones*[1322].

642. Le laboratoire d'Innovation Numérique de la CNIL. La CNIL, tout en étudiant les impacts de la technologie sur la gouvernance et sur la protection des données à caractère personnel, a également créé au sein de la direction des technologies et de l'information un laboratoire procédant à la conduite de projets d'expérimentation. Baptisé LINC (Laboratoire d'Innovation Numérique de la CNIL), ce laboratoire est un dispositif « de réflexion, d'information et de partage sur les tendances émergentes d'usage du numérique et des données » qui participe à la conduite « de projets d'expérimentation et de prototypage d'outils, de services ou de concepts autour des données »[1323]. Il cherche notamment à créer des liens entre les différents acteurs du numérique et il procède à des expérimentations centrées sur l'usage des données, permettant de rendre accessible des notions techniques parfois difficiles d'accès. Le LINC a par exemple contribué au développement d'une plateforme ouverte de cartographie du *privacy by design*, « afin d'explorer les stratégies mises en place par les acteurs les plus investis dans la protection des données personnelles et des libertés »[1324]. La CNIL précise explicitement qu'il s'agit d'une expérimentation et non d'une labellisation, enlevant tout doute sur sa portée juridique. Ce type d'expérience, parmi lesquelles on peut mentionner le développement d'un outil intitulé *Cookieviz*, permettant de visualiser les cookies déposés lors de la navigation sur Internet, permet une meilleure compréhension des enjeux techniques relatifs à la protection des données.

643. La sensibilisation aux risques. En lien direct avec les applications utilisés dans le cadre de l'automesure connectée, la CNIL s'est associée à une équipe de recherche de l'Inria afin de se doter d'un outil d'analyse des « flux de données

[1321] CNIL, *Vie privée à l'horizon 2020, Paroles d'experts*, Cahiers Innovation & Prospective, n° 1, novembre 2012.
[1322] CNIL, « Smartphones et vie privée : pour une nouvelle vision de la protection des données ? », Lettre Innovation & Prospective de la CNIL, n°2, février 2012.
[1323] Voir notamment le site du laboratoire : https://linc.cnil.fr/
[1324] https://linc.cnil.fr/fr/design-de-la-privacy-une-cartographie-de-veille-enrichir

entrant et sortant lors de l'utilisation en vie réelle des applications mobiles »[1325]. A ce titre, le projet de recherche initié a permis de mettre en lumière, à travers l'analyse des modes de fonctionnement des applications, les utilisations concrètes des données à caractère personnel collectées. Les problématiques relatives à la géolocalisation, aux différentes utilisations des identifiants des individus et aux divergences de finalité entre les accès aux données des individus et les buts poursuivis par les applications ont ainsi été relevées. Le but de cette expérimentation n'était pas de sanctionner directement les responsables de traitement, mais de rendre visible aux plus grand nombre les éventuels risques qui sont courus lors de l'utilisation d'applications de *smartphones* et dès lors de sensibiliser les personnes concernées par des traitement, mais également les responsables de traitement eux-mêmes.

Le rôle pédagogique de la CNIL et de son laboratoire d'innovation permet ainsi de contribuer à l'instauration d'une culture de la protection des données à caractère personnel, sans forcément avoir recours à une logique coercitive, la protection juridictionnelle appliquée ayant par ailleurs de plus en plus tendance à être externalisée.

§2. Une protection juridictionnelle externalisée

644. A l'image de l'internationalisation croissante des traitements de données à caractère personnel, les litiges portant sur ces traitements ont logiquement eu tendance à s'internationaliser. Les jurisprudences de la Cour européenne des droits de l'homme et de la Cour de justice de l'Union européenne ont progressivement pris une place importante dans le dispositif protecteur appliqué aux données. Conscientes des risques que le développement massif de l'informatique est susceptible de faire naître au regard des droits et libertés des individus, ces cours ont développé une jurisprudence extensive allant dans le sens d'une protection renforcée. Elle précise les différentes normes supranationales applicables, au regard notamment du fort niveau d'harmonisation de la matière en Europe, tant par le droit issu de la Convention

[1325] Voir notamment : CNIL, « Les smartphones et leurs apps sous le microscope de la CNIL et d'Inria », *Lettre Innovation & Prospective de la CNIL*, n°8, novembre 2014.

européenne des droits de l'Homme que par le droit de l'Union européenne[1326]. Ce rôle croissant qui a progressivement été conféré aux juridictions européennes **(A)** est pourtant susceptible d'être limité par l'absence remarquée de cadre international commun **(B)**.

A. Le rôle croissant des juridictions européennes

645. Le droit à la protection des données à caractère personnel s'est progressivement affirmé, au niveau européen, comme étant un droit fondamental nécessitant une protection renforcée. L'article 8 de la Charte des droits fondamentaux de l'Union européenne le consacre expressément, indiquant que « toute personne a droit à la protection des données à caractère personnel la concernant ». Cette affirmation est le fruit d'une évolution progressive du cadre juridique européen, dont l'adoption de la Convention 108 du Conseil de l'Europe, premier instrument international juridique contraignant dans le domaine de la protection des données, constitue le point de départ. Or, ce droit fait également l'objet d'une protection au titre de l'article 8 de la Convention européenne des droits de l'homme qui traite du droit au respect de la vie privée et familiale, du domicile et de la correspondance. Ainsi, entre droit de l'Union et droit du Conseil de l'Europe, la protection des données à caractère personnel fait l'objet d'une double protection au niveau européen, entraînant la compétence d'une dualité d'ordres juridictionnels. Ceux-ci, tout en contribuant à l'interprétation des règles **(1)** permettent d'apporter des garanties contre la surveillance de masse, exacerbée par le recours aux objets connectés utilisés pour la pratique du quantified-self **(2)**.

1. Une fonction d'interprétation

646. La Cour Européenne des Droits de l'Homme ainsi que la Cour de Justice de l'Union européenne ont toutes deux contribué à l'interprétation des notions dégagées par les différents textes européens, en commençant par la notion de données à caractère personnel elle-même.

[1326] Julien Rossi, « Guide de la jurisprudence européenne en matière de protection des données à caractère personnel », *Cahiers Costech*, mai 2017, n°1, p. 5.

Ainsi dans une affaire Amann[1327], la CEDH a interprété le terme « données à caractère personnel » comme n'étant pas « limité aux affaires de la sphère privée d'un individu »[1328]. Par ailleurs, la Cour de justice a indiqué dans un arrêt Volker und Markus Schecke et Hartmut Eifert c. Land Hessen que les termes « vie privée » ne devaient pas être interprétés de façon restrictive et qu'ils pouvaient donc comprendre les activités professionnelles[1329].

Outre des précisions sur la notion de données à caractère personnel, le spectre des données sensibles ou des catégories particulières de données a également été précisé. Ainsi, dans un arrêt *Bodil Lindqvist* touchant particulièrement le *quantified-self,* la CJUE a précisé que « l'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé, au sens de l'article 8, paragraphe 1, de la directive 95/46 »[1330]. Cette indication, anticipant la définition large des données de santé retenue par le RGPD, a permis de préciser la nature de certaines des données collectées par des dispositifs de *quantified-self,* les données relatives à certaines blessures devant être considérées comme des données sensibles.

647. Le dispositif protecteur est ainsi renforcé par l'interprétation qui est faite des termes de la réglementation. La Cour de justice a ainsi retenu une définition extensive de la notion de donnée à caractère personnel, au regard notamment des évolutions technologiques : registre de temps de travail[1331], images enregistrées dans le cadre de dispositifs de vidéosurveillance[1332] mais surtout adresses IP[1333] et métadonnées[1334], conformément au principe selon lequel une donnée à caractère personnel permet l'identification indirecte de l'utilisateur. Ainsi, malgré certaines

[1327] CEDH, *Amann c. Suisse*, n° 27798/95, 16 février 2000, paragraphe 65.
[1328] Conseil de l'Europe, *Manuel de Droit européen en matière de protection des données*, Agence des droits fondamentaux de l'Union européenne, 2014, p. 45.
[1329] CJUE, affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen*, 9 novembre 2010, para. 59
[1330] CJUE, C-101/01, *Bodil Lindqvist*, 6 novembre 2003, paragraphe 51, *D.* 2004. 1062, obs. L. Burgorgue-Larsen ; *RSC* 2004. 712, obs. L. Idot ; CJUE 6 nov. 2003, aff. C-101/01, *Lindqvist*, pt 27.
[1331] CJUE, C-342/12, *Worten contre ACT*, 30 mai 2013.
[1332] CJUE, C-212/13, *Frantisek Rynes*, 11 décembre 2013, paragraphe 21.
[1333] CJUE, C-70/10, *Scarlet Extended*, 24 novembre 2011, Rec. I. 11959 ; ECLI :EU :C :2011 :771.
[1334] CJUE, C-203/15 et C-698/15, *Tele2 Sverige*, 21 décembre 2016, paragraphe 97 à 100, aff. C-203/15, Dalloz actualité, **2** janv. 2017, obs. M.-C. de Montecler ; *AJDA* 2016. 2466 ; *ibid*. 2017. 1106, chron. E. Broussy, H. Cassagnabère, C. Gänser et P. Bonneville ; *D.* 2017. 8 ; *ibid*. 2018. 1033, obs. B. Fauvarque-Cosson et W. Maxwell ; *Dalloz IP/IT* 2017. 230, obs. D. Forest ; *RTD eur*. 2017. 884, obs. M. Benlolo Carabot ; *ibid*. 2018. 461, obs. F. Benoît-Rohmer ; *Rev. UE* 2017. 178, étude F.-X. Bréchot.

limites, concernant l'adresse IP notamment[1335], la tendance dégagée par la Cour s'inscrit dans le sens d'une appréciation large des termes employés par la réglementation.

648. Deux arrêts ont à ce titre contribué à établir un environnement protecteur des données à caractère personnel au niveau européen. L'arrêt *Google Spain*[1336] permettant l'instauration d'un droit au déréférencement, plus communément appelé droit à l'oubli, est particulièrement révélateur de ces évolutions. Précisant non seulement la qualification de responsable de traitement appliqué aux moteurs de recherche, cet arrêt permet de faire prévaloir les droits fondamentaux d'une personne sur l'intérêt économique de l'exploitant du moteur du recherche en appréciant la nécessité de la conservation des données par rapport au principe de finalité. Une partie de la doctrine a relevé que la CJUE a dû avoir « recours à une interprétation libérale de la directive » afin de retenir la responsabilité de l'exploitant du moteur de recherche[1337] mais la solution retenue s'est engagée dans la voie d'une protection accrue des individus tout en anticipant la question du droit au déréférencement consacrée par le RGPD. Le rôle protecteur de la Cour de justice a été confirmé par l'arrêt *Schrems* ayant conduit à l'invalidation de la décision de la Commission constatant que les Etats-Unis assuraient un niveau de protection adéquat aux données à caractère personnel transférées[1338]. L'annulation du *Safe Harbor* par la Cour de justice dans le cadre de ce renvoi préjudiciel montre que celle-ci s'engage dans la voie d'une protection renforcée des citoyens européens, notamment à l'égard de la surveillance de masse.

2. La fonction protectrice des droits fondamentaux

649. Le juge des droits fondamentaux. Les cours européennes orientent majoritairement leurs travaux sur les traitements réalisés par des personnes publiques ou, du moins, sur les aspects institutionnels liés à la protection des données à

[1335] Voir notamment : CJUE, C-582/14, *Breyer c. Allemagne*, 19 octobre 2016.
[1336] CJUE, C-131/12, *Google Spain, S.L., Google Inc. c. Agencia Española de Protección de Datos, Mario Costeja González*, 13 mai 2014.
[1337] Voir notamment : Marion Polidori, « L'arrêt Google Spain de la CJUE du 13 mai 2014 et le droit à l'oubli », *Civitas Europa*, vol. 34, no. 1, 2015, pp. 243-266.
[1338] CJUE, C-362/14, *Maximilian Schrems c. Data Protection Commissioner*, 6 octobre 2015.

caractère personnel. A ce titre, la Cour de justice de l'Union s'est rapidement engagée dans la voie d'une protection renforcée des individus, à l'égard notamment d'éventuels possibilités de surveillance généralisée. Celle-ci s'affirme en effet progressivement en tant que juge des droits fondamentaux en faisant le lien entre protection des données à caractère personnel et protection de tels droits. Deux décisions rendues le 8 avril 2014 sont révélatrices de la position adoptée par la Cour de justice, relatives d'une part à l'indépendance des autorités de protection nationales et d'autre part, à l'invalidité de la directive 2006/24 relative à la conservation des données.

La première décision est une constatation en manquement à l'encontre de la Hongrie pour violation de la directive 95/46/CE[1339]. Le commissaire hongrois à la protection des données ayant été démis de ses fonctions à l'occasion d'une réforme du dispositif national de protection des données, la Cour a pu rappeler que l'exigence d'indépendance de l'autorité de contrôle suppose « 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 ». Cette décision est surtout l'occasion pour la Cour de faire le lien direct entre protection des données personnelles et protection des droits fondamentaux[1340], sachant selon le point 47 de la décision que « l'exigence de contrôle par une autorité indépendante du respect des règles de l'Union relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel résulte également du droit primaire de l'Union, notamment de l'article 8, paragraphe 3, de la charte des droits fondamentaux de l'Union européenne ».

650. La prohibition de la surveillance. Le lien avec les droits fondamentaux est confirmé par la décision rendue le même jour et qui concerne la validité de la directive 2006/24/CE relative à la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au

[1339] CJUE, C-288/12, *Commission contre Hongrie*, grande chambre, 8 avril 2014.
[1340] Marie-Laure Basilien-Gainche, « Une prohibition européenne claire de la surveillance électronique de masse », *CDPH*, 15 mai 2014, accessible en ligne à cette adresse : http://combatsdroitshomme.blog.lemonde.fr/2014/05/15/une-prohibition-europeenne-claire-de-la-surveillance-electronique-de-masse-cjue-gc-8-avril-2014-digital-rights-ireland-ltd-michael-seitlinger-e-a/

public ou de réseaux publics de communications[1341]. La Cour, dans un contexte de révélation de pratiques de surveillance des individus par la *NSA* aux Etats-Unis, prononce l'invalidité de ce texte qui impose aux opérateurs de télécommunications et fournisseurs d'accès à Internet, de conserver pour une durée de six mois à deux ans un ensemble de données à caractère personnel. Cette décision, qui permet de s'affranchir de la jurisprudence de la CEDH[1342], s'appuie directement sur les articles 7 et 8 de la Charte des droits fondamentaux de l'Union pour caractériser l'ingérence « d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel ». Cette solution, confirmée par la suite[1343], interdit la conservation généralisée des données et par conséquent, met un frein à la « surveillance de masse » organisée par certains Etats[1344]. Cette solution doit être saluée, compte tenu du déploiement massif d'objets connectés permettant une collecte de données sans précédents. Ces données, par leur nombre et leur précision, pourraient devenir une source privilégiée de la surveillance. La solution retenue par la Cour montre que celle-ci entend interdire de telles pratiques.

Le lien entre vie privée et données à caractère personnel a d'ailleurs été confirmé par la Cour de Strasbourg. En effet, la CEDH a eu l'occasion, par certains arrêts, de confirmer le lien existant entre protection des données à caractère personnel et droit au respect de la vie privée. Ainsi, pour elle, « la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention », ce qui implique que « la législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article »[1345]. Les données à caractère personnel d'un individu sont donc une composante de sa vie privée. Ainsi, l'approche européenne

[1341] CJUE, C-293/12 & C-594/12, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*
[1342] Sylvie Peyrou, « La Cour de justice, garante du droit « constitutionnel » à la protection des données à caractère personnel », *RTD eur*., 2015, p. 117.
[1343] CJUE, 21 déc. 2016, aff. jtes C-203/15 et C-698/15, *Tele2 Sverige et Watson e.a*.
[1344] David Forest, « Conservation des données de connexion et métadonnées : un nouveau coup de semonce à la surveillance de masse en Europe », *Dalloz IP/IT*, 2017, p. 230.
[1345] CEDH, *S. et Marper c. Royaume-Uni*, arrêt (Grande Chambre) du 4 décembre 2008, §103, *RSC 2009. 182, obs.* Marguénaud *; RDIP 2009. 910, obs.* Gonzalez *; JCP* 2009. I. 104, nº 10, obs. Sudre ; *AJ pénal* 2009. 81, obs. Roussel ; *Dr. pénal* 2009. Chron. 4, obs. Dreyer.

unifiée de la protection des données à caractère personnel a tenu, contrairement à l'approche américaine reposant sur la notion de *privacy*, à définir un régime de protection spécifique pour les données personnelles, plus précis que celui reposant sur la protection de la vie privée. L'appréciation d'une violation de la règlementation repose donc sur un élément objectif et légalement déterminé, à l'inverse d'une appréciation relative à la vie privée, subjective et dont les critères pourraient varier en fonction des individus.

651. Pourtant, il pourrait être envisageable, pour des questions de simplicité, de revenir à une protection fondée sur l'atteinte à la vie privée des individus. En effet, la distinction entre problématiques relatives à la vie privée au sens large d'une part et problématiques relatives au numérique d'autre part, pourrait être remise en question. Comme le soulèvent certains auteurs, traiter plus largement du privé à l'image du concept anglo-saxon de *privacy*, permet de traiter de ce qui relève du privé, à la fois dans sa substance sociohistorique et en lien avec les problématiques technologiques, ce que le choix tranché entre l'un ou l'autre de ces champs ne permettrait pas de saisir dans sa globalité[1346]. Pour une application de *quantified-self*, l'atteinte ne sera plus caractérisée par le manquement à la loi Informatique et Libertés – le fait par exemple de conserver des données une fois la finalité du traitement réalisée – mais par le fait qu'un individu considérera qu'une atteinte a été portée à sa vie privée. Revenir à une conception large de la protection des données à caractère personnel, telle qu'elle peut également être entendue par le droit au respect de la vie privée et par la *privacy*, permettrait de dépasser certaines des limites propres aux principes classiques de la règlementation repris par le RGPD. Ces considérations, qui peuvent être écartées au regard de la technicité de la matière et des objets techniques nouveaux utilisés, sont en revanche symptomatiques de l'absence de cadre commun et international de protection des données à caractère personnel.

B. L'absence de cadre international commun

652. Le RGPD vise l'instauration d'un cadre européen harmonisé de protection des données à caractère personnel. L'emploi d'un règlement au profit d'une directive

s'inscrit ainsi dans cette optique d'uniformisation de la règlementation. Le recours à cet instrument juridique permet une protection homogène des individus sur le territoire européen mais la portée de ces règles protectrices peut néanmoins paraître dérisoire au regard de la spécificité du cyberespace. Le Règlement dispose en théorie d'une portée territoriale élargie mais celui-ci n'a pas vocation à protéger les individus non-ressortissants de l'Union lorsque des traitements sont réalisés hors du territoire de l'Union. Dès lors, les utilisateurs d'un même service pourront être soumis à deux régimes juridiques distincts. Un individu utilisant un service de *quantified-self* en France ne sera ainsi pas soumis à la même réglementation qu'un individu utilisant le même service outre-Atlantique. L'absence de cadre international commun, susceptible de conduire à une protection fragmentée des individus **(1)** commence cependant à laisser place à un début de coopération au niveau international **(2)**.

1. Une protection fragmentée

653. L'absence d'unité de la protection. Le cyberespace se caractérise par son absence de frontières terrestres physiques. Pourtant, celui-ci est à l'heure actuelle réglementé par des législations territorialement définies et limitées, susceptibles d'accorder des niveaux de protection différents aux individus. Le cas des Etats-Unis mérite à ce titre une attention toute particulière en raison du nombre de responsables de traitements qui y sont établis. Qu'il s'agisse notamment des GAFAM (Google, Amazon, Facebook, Apple, Microsoft) ou d'entreprises spécialisées dans le domaine du *quantified-self*, ils sont soumis à une législation présentant des différences notables avec le système de protection harmonisé en vigueur au niveau européen. Plusieurs différences majeures opposent en effet les Etats-Unis et l'Union européenne en matière de protection des données personnelles et de la vie privée et on constate que « la protection dans l'Union européenne est dite « omnibus », alors que le droit états-unien propose une approche sectorielle de la privacy »[1347]. Cette approche sectorielle s'est développée grâce à l'dentification de quatre catégories de comportements portant atteinte à la vie privée et découlant du droit de la

[1346] Voir notamment : Céline B. Rey, *La vie privée à l'heure du numérique*, Lavoisier, 2012, 304 p.

responsabilité civile extracontractuelle, communément appelée *torts law*[1348] : publication de faits appartenant à la vie privée, intrusion dans l'intimité, présentation d'une personne sous un jour défavorable ou trompeur, appropriation du nom ou de la ressemblance d'une personne.

Cette protection, variable car subjective, est susceptible d'entraîner un déséquilibre, en fonction du lieu où le traitement de données à caractère personnel est réalisé. En effet, le système fédéral contribue à la fragmentation du droit à la protection des données ; les fondements même de la protection diffèrent. La *privacy* n'est en effet pas considérée comme un système de protection uniformisé à l'image du système européen[1349]. Ce concept, identifié à la fin du XIXème siècle[1350] et reconnu par la Cour suprême en 1965[1351], relève ainsi des législations de chaque Etat ainsi que de son application et interprétation par les différentes juridictions.

654. La protection limitée. Aux Etats-Unis, le 4ème Amendement de la Constitution garantit seulement un droit à la protection de la vie privée à l'égard du gouvernement. Les lois fédérales développées par suite de l'adoption du *Privacy Act* de 1974 ne réglementent que certains secteurs privés[1352] et la FTC protège les données à caractère personnel sur le fondement des pratiques déloyales. Ainsi, l'absence d'harmonisation du cadre de la protection des données au niveau international génère des difficultés, en particulier au regard du développement du *quantified-self* et des objets connectés. L'invalidation du *Safe Harbor* ainsi que les critiques formulées à l'encontre du *Privacy Shield* n'ont pas permis de restaurer la confiance à l'égard du niveau de protection adéquat conféré par la réglementation américaine. En effet, les avancées qu'il devait permettre semblent limitées dès lors que la portée de la collecte peut par exemple toujours être justifiée « à des fins de « sécurité nationale », un motif comprenant des objectifs aussi larges que non-

---

[1347] Paul M. Schwartz et Daniel J. Solove, *Information Privacy Law*, 5e éd., Wolters Kluwer, p. 1134.
[1348] Céline Castets-Renard, article précité, p. 356.
[1349] Céline 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.
[1350] Samuel Warren et Louis Brandeis, *The Right to Privacy*, Harvard Law Review, Vol. IV, Dec. 15, 1890, n° 5.
[1351] Griswold v. Connecticut, 381 U.S. 479 (1965).
[1352] Voir par exemple l'HIPAA (Health Insurance Portability and Accountability Act) concernant la protection des données de santé ou l'ECPA (Electronic Communications Privacy Act) visant la protection des données de télécommunications.

définis »[1353]. Les problématiques relatives à l'accès, par des agences étrangères, aux données d'individus issues d'objets connectés doit être soulevée, au regard notamment du nombre et de la précision des informations traitées. La question peut également être envisagée sous un aspect concurrentiel, la souplesse des règles américaines étant susceptible d'entraîner une perte de compétitivité pour les entreprises européennes.

655. Les limites du *Privacy Shield*. Certaines instances européennes se prononcent en faveur d'une renégociation du *Privacy Shield*[1354] ou même d'une suspension pure et simple d'un tel accord[1355]. Il faut pourtant constater que des évolutions de la réglementation américaine en matière de protection des données à caractère personnel ont été envisagées. Celles-ci, annoncées sous l'administration Obama, devaient permettre une application uniforme de règles protectrices de données à caractère personnel, à l'image du *Personal Data Notification & Protection Act* visant à établir une norme commune à laquelle les entreprises peuvent adhérer en cas d'incidents en matière de données à caractère personnel. Ces tentatives de législation n'ont pourtant pas pu aboutir. Elles ont en revanche laissé place à l'adoption d'une nouvelle loi, le *Cloud Act* (Clarifying Lawful Overseas Use of Data Act). Celui-ci permet aux autorités américaines « d'obtenir de toute société « de droit américain » détenant des data centers en dehors des Etats-Unis, la divulgation de données dans le cadre d'investigations criminelles », permettant ainsi aux administrations d'avoir accès à des données « sans considération du lieu où se trouvent celles-ci »[1356]. Ce texte, qui fait obligation aux entreprises américaines de fournir des données d'utilisateurs même lorsqu'elles sont stockées ou qu'elles transitent à l'étranger, ne s'oppose pas directement aux termes du RGPD. Mais les entreprises soumises au droit européen vont devoir faire preuve de vigilance lorsqu'elles choisissent des prestataires de *cloud* situées aux Etats-Unis. En effet, ces entreprises vont devoir intégrer, « dans leur cartographie des risques découlant de

[1353] Conseil National du Numérique, *Pourquoi le Privacy Shield doit être renégocié*, Communiqué, 19 septembre 2017.
[1354] European Parliament, Draft Motion for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-U.S. Privacy Shield (2018/2645(RSP)), Committee on Civil Liberties, Justice and Home Affairs, 10.4.2018.
[1355] European Parliament, « EU-US Privacy Shield data exchange deal : US must comply by 1 September, say MEPs », 12.06.2018, Press Releases.
[1356] Flora Plénacoste, Emmanuel Daoud, « *Cloud Act* : des inquiétudes légitimes », *Dalloz IP/IT*, 2018, p. 680.

l'externalisation de leurs données, la nationalité du prestataire pressenti afin de contenir le risque de communication de données dans le cadre d'une enquête diligentée par des autorités américaines » [1357].

L'influence du RGPD sur la réglementation internationale ne doit, de manière générale, pas être occultée. Le cadre protecteur commun qu'il met en œuvre ainsi que la confiance qu'il est susceptible d'apporter aux utilisateurs de différents services est révélateur du début de coopération à l'œuvre sur la question de la protection des données à caractère personnel.

2. Un début de coopération

656. Le RGPD, doté d'une compétence territoriale large, a vocation à s'appliquer lorsqu'un responsable de traitement ou un sous-traitant est établi sur le territoire de l'Union, mais également lorsque le traitement concerne une personne qui se trouve sur le territoire de l'Union. L'internationalisation des services proposés, dans le cadre du *quantified-self* notamment, a pour effet de soumettre un certain nombre de responsables de traitement ou de sous-traitants étrangers à la réglementation européenne, dès lors que les traitements concernent des individus qui se situent sur le territoire européen. Malgré les différences conceptuelles entre les législations internationales, le RGPD aura donc vocation à influencer la façon dont les traitements seront mis en œuvre par des responsables de traitement étrangers. Ainsi, le champ d'application territorial élargi du RGPD pourrait avoir un écho positif au sein des entreprises situées outre-Atlantique. Des services ont été contraints de limiter ou de bloquer l'accès à leurs sites en Europe en attendant que la conformité au Règlement soit établie. Mais, l'adoption de mesures de conformité par l'ensemble des responsables de traitement, pourrait ainsi avoir une influence sur ceux mis en œuvre outre-Atlantique, au niveau simplement national.

657. Le domaine des objets connectés est particulièrement propice au développement de normes internationales communes. Les modalités d'interaction de

[1357] Corinne Thierache, « RGPD vs. *Cloud Act* : le nouveau cadre légal américain est-il anti-RGPD ? », *Dalloz IP/IT*, 2019, p. 367.

ces objets, les capacités de croisement des données ou encore le recours systématique au *cloud* pour le stockage font que ceux-ci pourraient particulièrement bénéficier d'un cadre commun leur accordant un socle partagé de régulation. Des discussions récentes au sein de la Commission européenne semble s'orienter en ce sens. Celle-ci recommandait, dans une communication relative au marché unique numérique, de s'engager sur l'adoption de normes relatives à l'Internet des objets, notamment en matière de sécurité et d'interopérabilité[1358]. Andrus Ansip, vice-président de la Commission européenne en charge des politiques numériques a, à ce titre, appelé à la création d'une zone de « cybersécurité transatlantique » avec les Etats-Unis. Celle-ci ne concerne pas directement le cadre des données personnelles mais elle doit permettre la création d'éléments de réglementation visant à garantir la sécurité des données traitées. Ces discussions ainsi que l'accord qui en découlerait permettrait aux normes de sécurité adoptées au niveau de l'Union européenne d'être également intégrées par d'autres Etats[1359].

658. Sans pour autant considérer que la nouvelle réglementation européenne soit un modèle à adopter au niveau mondial, en raison notamment des limites pratiques déjà exposées et relatives à certains principes fondamentaux de la collecte, le développement d'un cadre protecteur commun doit être encouragé. Une telle globalisation ou mondialisation du droit à la protection des données à caractère personnel semble en effet nécessaire. En effet, si ce sont le plus souvent les crises qui déclenchent ce processus[1360], celle que connaît le droit à la protection des données à caractère personnel depuis les premières révélations d'Edward Snowden en 2013 en passant par l'affaire Cambridge Analytica en 2018, justifie que des mesures globales soient adoptées afin de protéger au mieux les libertés individuelles. A ce titre, l'idée d'une convergence des droits doit être privilégiée, à travers l'harmonisation ou encore l'unification des normes juridiques[1361]. Le domaine du numérique s'y prête particulièrement, en raison notamment des questions soulevées par l'identification de

[1358] European Commission, *A Digital Single Market Strategy for Europe*, Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM (2015) 192 final, Brussels, 6.5.2015.
[1359] Catherine Stupp, « Ansip évoque des normes communes de cybersécurité avec les Etats-Unis », Euractiv, 20 avril 2018, disponible en ligne : https://www.euractiv.fr/section/economie/news/ansip-surprises-with-proposal-to-step-up-work-with-us-on-cybersecurity/
[1360] Mireille Delmas-Marty, « La mondialisation du droit : chances et risques », *Recueil Dalloz*, 1999, p. 43.
[1361] Marie-Claire Ponthoreau, « Trois interprétations de la globalisation juridique », *AJDA*, 2006, p. 20.

la loi applicable[1362]. Cette « extension à l'échelle du monde de la règle de droit comprise au sens de codification normative des relations de confiance »[1363] devrait ainsi permettre une appréhension globale de la matière et surtout garantir que les droits des individus soient protégés au niveau mondial, protection que les objets connectés utilisés pour la pratique de l'automesure mettent à mal.

659. Conclusion du chapitre. La responsabilisation des acteurs du numérique, responsables de traitement d'automesure, s'accompagne du rôle grandissant d'un certain nombre d'agences et d'autorités. Sans pour autant conclure à un aveu d'impuissance de la part de l'Etat face à la mise en œuvre généralisée de traitements de données, le recours à des organismes spécialisés permet aux opérateurs du numérique une meilleure appréhension des problématiques spécifiques au *quantified-self*. Le recours à ces tiers est dans certains cas encouragé par le RGPD qui vise à favoriser les mécanismes de certification permettant d'attester du niveau de conformité à la réglementation.

Ces différents éléments permettent de confirmer que la nature du droit a vocation à changer lorsqu'il est confronté aux évolutions technologiques. Comme le révèlent certains auteurs, le droit « a tendance à devenir « mou » au contact du numérique et à se mettre ainsi au service de la régulation et de l'imprévisibilité »[1364]. Ayant pour objectif de faire en sorte que les acteurs soient de plus en plus impliqués dans la mise en place de pratiques respectueuses[1365], le recours à la régulation constitue aujourd'hui une réponse pertinente aux modifications des pratiques permises par l'automesure. Les responsables de traitement semblent en effet plus enclins à appliquer des règles qu'ils ont contribué à créer, en concertation avec d'autres organismes. Ce phénomène permet de confirmer qu'il n'existe plus un droit unique de la protection des données, mais des droits de la protection des données, adaptés aux spécificités des traitements mis en œuvre, y compris dans le cadre du *quantified-self*.

[1362] Jean-Bernard Auby, *La globalisation, le droit et l'Etat*, LGDJ, Systèmes, 2010, p. 33.
[1363] Zaki Laïdi, « Mondialisation et droit », *Recueil Dalloz*, 2007, p. 2712.
[1364] Karine Favro, *op. cit.*, p. 11.
[1365] Régis Lanneau, « Le normal et le pathologique dans la régulation, un vertige épistémologique », *in* Sée A., *Régulations*, 2013, Editions La Mémoire du Droit, p. 21.

660. Conclusion du titre. Les technologies novatrices ayant vu le jour ces dernières années (smartphones, tablettes, objets connectés) ont entraîné l'apparition de nouveaux services (réseaux sociaux, applications mobiles, *quantified-self*) reposant sur des collectes sans précédent de données à caractère personnel. Ces technologies semblent, à l'origine, avoir occulté les problématiques relatives à la collecte généralisée de données identifiantes en raison des avantages conférés par les différents services proposés. Le RGPD tente, en consacrant certaines mesures nouvelles, de rétablir un équilibre entre les enjeux économiques associés aux traitements de données et les impératifs relatifs à la protection de telles informations. Ce faisant, le texte européen s'engage dans le sens d'une rationalisation des services fondés sur la révélation de données identifiantes. Les problématiques soulevées par notre étude, relative à la classification des données collectées – données personnelles et données de santé – et à leur régime juridique protecteur, ont ainsi vocation à s'effacer au profit d'éléments de protection sur mesure, adaptés à la nature des données traitées.

Le RGPD, en impliquant les responsables de traitement dans la mise en œuvre de solutions protectrices, entend procéder à une reconstruction du cadre juridique. Cette reconstruction, qui passe par le recours à des éléments empruntés à la régulation, conduit à la mise en œuvre d'éléments originaux de protection, entre renouvellement de principes protecteurs éprouvés et recours à des instruments de droit souple. La solution adoptée doit permettre, après un premier temps d'adaptation nécessaire, une protection efficace des traitements réalisés dans le cadre de l'automesure : les spécificités techniques des traitements d'automesure ainsi que le poids économique des opérateurs font que ces derniers doivent avoir une place centrale dans la mise en œuvre du dispositif protecteur. En donnant la possibilité aux responsables de traitement de définir eux-mêmes certains éléments de protection, tout en renforçant les pouvoirs de contrôle et de sanction des autorités administratives, le RGPD contribue ainsi à la mise en œuvre d'une protection mieux adaptée.

661. Conclusion de la partie. La pratique de l'automesure connectée a fragilisé, par les différentes opérations mises en œuvre, le cadre juridique protecteur des données à caractère personnel. Les spécificités propres aux traitements de

quantified-self ont donc nécessité qu'une réponse originale soit apportée pour permettre la maîtrise du risque informationnel. Deux mouvements complémentaires et convergents ont été mis en œuvre. D'une part, un renouvellement et un élargissement des mécanismes protecteurs préexistants afin de mieux prendre en compte les acteurs appelés à traiter des données, peu importe leur lieu d'établissement. D'autre part, la création ou la consécration de mécanismes novateurs visant à identifier les risques et à prévenir leur réalisation. Ainsi, la reconstruction du cadre juridique a nécessité une entente coordonnée entre différents acteurs appelés à jouer un rôle dans la protection des données à caractère personnel : législateur, autorités administratives indépendantes, agences, responsables de traitement et parfois même, personnes concernées par des traitements. Plutôt qu'un ensemble de règles de droit figées devant être appliquées strictement par les responsables de traitement, le système désormais en place repose sur une approche dynamique de la protection.

Cette approche dynamique et proactive de la protection, désormais encouragée, va de pair avec la spécificité des opérations réalisées. De la même manière qu'il n'existe pas de *quantified-self* unique et standardisé, il ne peut y avoir de réponse unique apportée aux différents traitements. Le dispositif protecteur doit en effet, pour protéger efficacement les individus, pouvoir s'adapter aux spécificités de chaque opération d'automesure. Faire intervenir les différents acteurs concernés en ayant recours à différents instruments – parfois extra-juridiques – semble ainsi être la seule solution permettant d'apporter une protection satisfaisante aux différentes problématiques soulevées par le *quantified-self*. Ce dernier, par son originalité et par les différents objectifs qui lui sont assignés, implique nécessairement qu'une réponse novatrice soit apportée. Les éléments de réglementation et de régulation qui sont conjointement convoqués par le cadre juridique renouvelé permettent d'apporter des éléments de maîtrise du risque informationnel.

Ces éléments, par le changement de paradigme qui est impliqué, nécessiteront que les différents acteurs puissent s'adapter aux nouvelles règles à appliquer. Les modalités de mise en œuvre de certains mécanismes protecteurs manquent encore de précision (dans le cas de la *privacy by design* par exemple) et des oppositions entre différents cadres juridiques pourraient apparaître (entre RGPD et *Cloud Act*

notamment). La CNIL, consciente du temps nécessaire à l'assimilation du changement de culture de la protection des données, avait d'ailleurs expressément indiqué que l'année 2018 serait une année de transition, le contrôle des exigences issues du nouveau texte étant reporté à l'année 2019[1366]. Une étude réalisée par l'institut de recherche de la société Capgemini montre pourtant que les entreprises ont pris du retard dans la mise en œuvre des mesures de conformité, 28% d'entre elles seulement indiquant être en conformité avec la réglementation[1367]. Une avancée doit cependant déjà être remarquée : les avantages concurrentiels que les entreprises peuvent tirer de leur conformité sont confirmés par cette étude, 81% de ces entreprises indiquant que la mise en œuvre des mesures issues du RGPD permet d'améliorer leur réputation et leur image.

[1366] CNIL, « Quelle stratégie de contrôle pour 2019 ? », 19 avril 2019, en ligne : https://www.cnil.fr/fr/quelle-strategie-de-controle-pour-2019
[1367] Capgemini Research Institute, *Championing Data Protection and Privacy, a source of competitive advantage in the digital century*, septembre 2019, 36 p.

Conclusion générale

662. Né du besoin de protéger les individus contre les traitements réalisés par l'administration, le droit à la protection des données à caractère personnel a rapidement fait l'objet d'évolutions visant à prendre en compte la valeur marchande des données. Les principes de base de la protection des données instaurés depuis la fin des années 1970 ont été conservés mais différentes réformes, procédant par petites touches, ont contribué à un ajustement des règles protectrices. La souplesse des termes employés par la réglementation, conformément au principe de neutralité technologique, a permis de laisser libre cours aux innovations, favorisant ainsi l'apparition de nouveaux services. Parmi ceux-ci, le *quantified-self* a joué un rôle particulier. En effet, sa pratique a contribué à révéler les limites du cadre juridique applicable aux traitements de données.

L'automesure a d'abord procédé à une remise en cause des principes de protection employés par la réglementation, qu'il s'agisse par exemple des principes de finalité déterminée ou de proportionnalité des traitements. Mais l'automesure a également permis de montrer en quoi l'approche du législateur, fondée sur l'actualisation de principes ayant vu le jour à l'heure où ces technologies n'existaient pas, n'était plus adaptée. Ainsi, plus qu'une simple fragilisation des principes de protection, le *quantified-self* et les outils utilisés pour sa pratique ont contribué à révéler les limites de l'appréhension des nouvelles technologies par le droit. La réforme d'ampleur instaurée par le RGPD, afin de garantir la maîtrise du risque informationnel, se devait d'adopter une approche radicalement différente des mécanismes protecteurs des données.

663. Le nouveau Règlement général européen, entré en application le 25 mai 2018, adopte une solution originale qui s'inscrit dans un mouvement de développement de la régulation. Des instruments de droit souple, directement prévus par le texte, contribuent à ce développement et favorisent également l'autorégulation des responsables de traitement. Les mécanismes instaurés constituent en théorie une

réponse satisfaisante aux problématiques posées par le *quantified-self*. Ils permettent en effet d'adapter les mesures protectrices à des situations différentes : les spécificités des traitements réalisés sont prises en compte pour apporter une protection adaptée aux données.

Notre étude permet de constater qu'une meilleure protection des données à caractère personnel est rendue possible par le nouveau texte européen. Mais le système de protection prévu par le RGPD, malgré des avancées certaines, laisse plusieurs questions en suspens. D'une part, certains instruments présentent d'ores et déjà des limites, à l'image de la *privacy by design* qui semble difficilement applicable au cas du *quantified-self*. La diversité et la souplesse des instruments déployés par le RGPD sont censées permettre de dépasser ces limites, mais les spécificités de l'automesure semblent, malgré tout, les rendre inopérants. D'autre part, la participation des responsables de traitement à la régulation pose la question d'une éventuelle concentration de cette régulation aux mains d'acteurs économiques devenus omnipotents. Les autorités administratives constituent une soupape de sécurité permettant d'éviter cette concentration et la pratique du RGPD devra éviter que le déplacement de la régulation s'accompagne de sa concentration, qui pourrait *in fine* servir les intérêts des responsables de traitement au détriment des individus.

664. L'adoption du RGPD, encore récente, ne permet pas de répondre à l'intégralité des questions juridiques soulevées par la pratique du *quantified-self*. Mais ce texte pourrait contribuer à redéfinir les standards internationaux de protection des données à caractère personnel. Le Japon et l'Union européenne ont par exemple signé, en juillet 2018, un accord visant à la création d'une zone de transfert sécurisée pour les données. La Californie, par suite de l'affaire dite *Cambridge Analytica*, a adopté une loi inspirée du texte européen censée garantir une protection renforcée des données à caractère personnel. Ces exemples, révélateurs de l'influence du RGPD, montrent que celui-ci pourrait constituer la première étape d'une prise de conscience généralisée des problématiques relatives à la protection des données. Si cette influence doit être saluée, seule l'instauration d'un cadre international commun de protection permettra cependant de protéger efficacement les données des individus.

665. La particularité des services numériques utilisés pour la pratique de l'automesure est de contribuer à une remise en question des frontières terrestres et à un éclatement du droit. Mais les limites relatives à l'extension du champ d'application du régime protecteur sont également liées aux enjeux économiques du *quantified-self*. Les Etats essaient d'asseoir leur souveraineté numérique par le droit : aux impérialismes juridiques européens ou américains s'oppose, par exemple, le protectionnisme chinois. Or, ces différents enjeux de souveraineté numérique contribuent aujourd'hui à renforcer l'antagonisme des conceptions de la vie privée au niveau mondial[1368]. Ainsi, la conclusion de notre étude ne peut aller que dans un sens : malgré les efforts réalisés pour développer des accords de coopération et pour parvenir à une certaine entente sur le sujet de la protection des données à caractère personnel, l'instauration d'un cadre harmonisé de protection nécessitera que des compromis soient réalisés sur ces enjeux de souveraineté. Ceux-ci permettront *in fine* aux services d'automesure de se développer en tenant compte, à tout moment, des questions relatives à la protection des données des individus.

[1368] Franck Montage, Gérard Longuet, *Le devoir de souveraineté numérique*, Rapport fait au nom de la commission d'enquête sur la souveraineté numérique, 1er octobre 2019, 253 p.

Bibliographie

I. OUVRAGES GENERAUX, TRAITES ET MANUELS

AUBY J.-M, DUCOS-ADER R., *Droit de l'information*, 2ème édition, Dalloz, 1982, 828 p.

BAZEX M., ECKERT G., LANNEAU R., LE BERRE C., MARAIS D.-B., SEE A. (dir.), *Dictionnaire des régulations 2016*, LexisNexis, 2015, 664 p.

BENABENT A., *Droit civil. Les obligations*, Montchrestien, Domat droit privé, 11ème édition, aout 2007, p. 21.

BENSOUSSAN A., *Informatique Télécoms Internet*, Francis Lefebvre, 6ème édition, 2017, 1392 p.

BERGEAL C., *Manuel de légistique*, Berger-Levrault, 8ème édition, 2018, 473 p.

BIOY X., *Droits fondamentaux et libertés publiques*, LGDJ, 5ème édition, 2018, 976 p.

BISMUTH Y., *Le droit de l'informatique*, 4ème édition, L'Harmattan, 2017, 430 p.

BLUMANN C., DUBOUIS L., *Droit institutionnel de l'Union européenne*, 6ème édition, LexisNexis, coll. Manuels, 2016, 922 p.

BLUMANN C., DUBOUIS L., *Droit matériel de l'Union européenne*, 7ème édition, LGDJ, coll. Précis Domat, 878 p.

BROYELLE C., *Contentieux administratif*, LGDJ, coll. « Manuels », 5ème ed., 2017, 540 p.

BURDEAU G., *Les libertés publiques*, 3ème édition, LGDJ, 1966, 422 p.

CABRILLAC R., FRISON-ROCHE M.-A., REVET T., *Droits et libertés fondamentaux*, 16ème édition, Dalloz, 2010, 860 p.

CAPRIOLI E., *Droit international de l'économie numérique*, LexisNexis, 2ème édition, 2007, 369 p.

CARBONNIER J., *Droit civil. Vol. 2 : Les biens, les obligations*, PUF, coll. « Quadrige », 2004, 2574 p.

CASTETS-RENARD C., *Droit de l'internet : droit français et européen*, LGDJ, 2ème édition, 2012, 492 p.

CHARVIN R., SUEUR J.-J., *Droits de l'homme et libertés de la personne*, LexisNexis, 5ème édition, Objectif Droit, 2007, 291 p.

CHEVALLIER J., *Science administrative*, PUF, 6ème édition, 2019, 636 p.

CHEVALLIER J., LOCHAK D., Science administrative, Tome I – Théorie générale de l'institution administrative, LGDJ, 1978.

CHEVALLIER J., LOCHAK D., Science administrative, Tome II – L'administration comme organisation et système d'action, LGDJ, 1978.

COLLIARD C.-A., *Libertés publiques*, 5ème édition, Dalloz, 1975, 839 p.

CORNU G., *Droit civil. Les personnes*, Montchrestien, 13ème édition, août 2007, p. 65.

CORNU G., *Droit civil. Les biens*, Montchrestien, 13ème édition, octobre 2007, p. 67.

CORNU G., *Vocabulaire juridique*, Paris, PUF, 11e édition, 2016, 1101 p.

CORNU M., ORSI F., ROCHFELD J. (dir.), *Dictionnaire des biens communs*, PUF, Dictionnaire Quadrige, aout 2017, 1252 p.

DEBBASCH C., ISAR H., AGOSTINELLI X., *Droit de la communication*, Dalloz, Précis, 2001, 927 p.

DE BELLESCIZE D., FRANCESCHINI L., *Droit de la communication*, 2ème édition, PUF, 2011, 704 p.

DENIZEAU C., *Droit des libertés fondamentales*, Vuibert, 2019, 432 p.

DUPRE DE BOULOIS X., *Droit des libertés fondamentales*, Paris, PUF, 2018, 550 p.

FAVOREU L. (dir.), *Droit des libertés fondamentales*, 7ème éd., Dalloz, coll. Précis, 2015, 774 p.

FAVRO K., *Droit de la régulation des communications numériques*, LGDJ, Lextenso, 2018, 158 p.

FERAL-SCHUHL C., *Cyberdroit ; le droit à l'épreuve de l'internet*, Dalloz, 7ème édition, 2018, 1852 p.

FIALAIRE J., MONDIELLI E., *Droits fondamentaux et libertés publiques*, Ellipses, 2005, 560 p.

FOREST D., *Droit des données personnelles*, Gualino, 2011, 118 p.

GENTOT M., *Les autorités administratives indépendantes*, LGDJ, coll. Clefs, 1994, 160 p.

GOHIN O., *Institutions administratives*, LGDJ, 2016, 576 p.

GRAWITZ M., *Méthodes des sciences sociales*, Dalloz, 11ème éd., coll. Précis, 2000, 1040 p.

HENNETTE-VAUCHEZ S., ROMAN D., *Droits de l'Homme et libertés fondamentales*, Dalloz, HyperCours, 1ère édition, 2013, 854 p.

HEYMANN-DOAT A., CALVES G., *Libertés publiques et droits de l'homme*, LGDJ, Systèmes, 2008, 288 p.

HUET J., DREYER E., *Droit de la communication numérique*, LGDJ, 2011, 384 p.

ISRAEL J.-J., *Droit des libertés fondamentales*, LGDJ, 1998, 596 p.

LATOUR X., PAUVERT B., *Libertés publiques et droits fondamentaux*, 3ème édition, Studyrama, 2011, 342 p.

LEBRETON G., *Libertés publiques et droits de l'homme*, Sirey, 8ème édition, 2008, 570 p.

LECLERCQ C., *Libertés publiques*, Litec, 5ème édition, 2003, 363 p.

LOMBARD M., DUMONT G., SIRINELLI J., *Droit Administratif*, Dalloz, coll. « HyperCours », 12ème éd., 2017, 686 p.

LUCAS A., *Le droit de l'informatique*, PUF, coll. « Thémis », 1987, 551 p.

LUCAS A., DEVEZE J., FRAYSSINET J., *Droit de l'informatique et de l'Internet*, PUF, coll. « Thémis », 2001, 748 p.

MADIOT Y., *Droits de l'homme et libertés publiques*, Masson, 1976, 298 p.

MILLARD E., *Théorie générale du droit*, coll. « Connaissance du droit », Dalloz, 2006, 136 p.

MORANGE J., *Droits de l'homme et libertés publiques*, PUF, 2000, 460 p.

OBERDORFF H., *Droits de l'Homme et libertés fondamentales*, LGDJ Lextenso Editions, 5ème édition, 2015, 688 p.

PLESSIX B., *Droit administratif général*, LexisNexis, coll. « Manuels », 2ème ed., 2018, 1648 p.

PRELOT J.-P., *Droit des libertés fondamentales*, Hachette Education, 2010, 320 p.

RENUCCI J.-F., *Droit européen des droits de l'homme*, 3ème édition, LGDJ, 600 p.

RIVERO J., *Les libertés publiques*, Tome I, PUF, coll. « Thémis », 1973, 273 p.

ROBERT J., *Libertés publiques*, Montchrestien, 1971, 651 p.

ROBERT J., DUFFAR J., *Droits de l'homme et libertés fondamentales*, Domat, Montchrestien, 8ème édition, 2009, 907 p.

ROCHFELD J., *Les grandes notions du droit privé*, coll. « Thémis », 2013, 592 p.

SUDRE F., *Droit européen et international des droits de l'homme*, PUF, 2016, 1005 p.

SUDRE F., MARGUENAUD J.-P., ANDRIANTSIMBAZOVINA J., GOUTTENOIRE A., LEVINET M., GONZALEZ G., *Les grands arrêts de la Cour européenne des droits de l'homme*, PUF, coll. « Thémis », 2011, 944 p.

TRUCHET D., *Droit administratif*, PUF, 2019, 520 p.

TURPIN D., *Libertés publiques & droits fondamentaux*, LGDJ, 2004, 623 p.

II. OUVRAGES SPECIALISES, THESES ET MONOGRAPHIES

AUBY J.-B., *La globalisation, le droit et l'Etat*, LGDJ, Systèmes, 2010, p. 33.

BABINET G., *L'Ere Numérique, Un Nouvel âge de l'humanité : cinq mutations qui vont bouleverser notre vie*, Le Passeur, janvier 2014, 236 p.

BALLANO BARCENA M., WUEEST C., LAU H., *How Safe is your Quantified-Self*, Symantec Security Response, 2014, p. 10.

BELLI L., *De la gouvernance à la régulation d'Internet*, Berger-Levrault, mars 2016, 457 p.

BENABOU V.-L., ROCHFELD J., *A qui profite le clic ?*, Odile Jacob, coll. Corpus, 2015, p. 20.

BENHOZI P.-J., BUREAU S., MASSIT-FOLLEA F., *L'internet des objets, quels enjeux pour l'Europe ?*, Editions de la Maison des sciences de l'homme, 2009, 170 p.

BELLANGER P., *La souveraineté numérique*, Stock, janvier 2014, p. 201.

BERNAL P., *Internet Privacy Rights, Rights to Protect Autonomy*, Cambridge University Press, 2014, 311 p.

BERTHIER T., TEBOUL B., *Des traces numériques aux projections algorithmiques*, Hermes Science Publishing Ltd, novembre 2018, 182 p.

BLANC-GONNET JONASON P., *Protection de la vie privée et transparence à l'épreuve de l'informatique (Droit français, droit suédois et directive 95/46/ce du Parlement européen et du Conseil du 24 octobre 1995)*, thèse, Paris XII, 2000, 580 p.

BOURCIER D., THOMASSET C., *L'écriture du droit …face aux technologies*, Diderot Editeurs, Arts et Sciences, 1996, 650 p.

BOURDIEU P., *Le sens pratique*, Les Editions de Minuit, 1er février 1980, 500 p.

BOURGEOIS M., *Droit de la donnée, Principes théoriques et approche pratique*, Communication et commerce électronique, LexisNexis, 2017, p. 76.

BOURGEOS C., *L'anonymat et les nouvelles technologies de l'information*, thèse, Paris V, 2003, 538 p.

CACHARD O., *La régulation internationale du marché électronique*, thèse, LGDJ, Bibliothèque de droit privé, Tome 365, 2002, 472 p.

CALANDRI L., *Recherche sur la notion de régulation en droit administratif français*, thèse, LGDJ, Bibliothèque de droit public, Tome 259, 2008, 752 p.

CARDON D., *A quoi rêvent les algorithmes, nos vies à l'heure des big data*, La République des Idées, Seuil, 2015, p. 11.

CARIAT N., *La Charte des droits fondamentaux et l'équilibre constitutionnel entre l'Union européenne et les Etats membres*, Collection du Centre des droits de l'homme de l'Université catholique de Louvain, Bruylant, 2016, p. 1042 p.

CASTILLO RUGELES J.-A., *La protection de la vie privée face au développement de l'informatique*, thèse, Paris I, 1975, 362 p.

CHEVALLIER J., *L'Etat post-moderne*, 4ème édition, LGDJ, décembre 2017, p. 14.

CHIGNARD S., BENYAYER L.-D, *Datanomics*, Editions Fyp, 2015, p. 17.

CLUZEL-METAYER L., *Le service public et l'exigence de qualité*, thèse, Dalloz, Nouvelle bibliothèque de Thèses, Volume 52, 2006, 634 p.

COLLET M., *Le contrôle juridictionnel des actes des autorités administratives indépendantes*, thèse, LGDJ, Bibliothèque de droit public, Tome 233, 2003, 398 p.

DEBAETS E., *Le droit à la protection des données personnelles, Recherche sur un droit fondamental*, Thèse pour obtenir le grade de docteur de l'Université Paris 1 Panthéon-Sorbonne, présentée et soutenue publiquement le 12 décembre 2014, p. 12.

DEBET A., MASSOT J., METALLINOS N., *La protection des données à caractère personnel en droit français et européen*, Lextenso Editions, 2015, 1296 p.

DEIBERT J.-R., *Black Code, Surveillance, Privacy, and the Dark Side of the Internet*, Signal McClelland & Stewart, 2013, 320 p.

DELMAS-MARTY M., *Le flou du droit*, PUF, 1986, 332 p.

DESGENS-PASANAU G., FREYSSINET E., *L'identité à l'ère numérique*, Dalloz, Présaje, 1ère édition, 2009, 170 p.

DESGENS-PASANAU G., *La protection des données personnelles*, Lexis Nexis, 2ème édition, 2015, p. 25.

DESGENS-PASANAU G., *La protection des données personnelles, Le RGPD et la nouvelle loi française*, 3ème édition, 2018, 250 p.

DESROSIERES A., *Pour une sociologie historique de la quantification. L'argument statistique I*, Presses de l'Ecole des mines, 2008, p. 10-11.

DUGAIN M., LABBE C., *L'homme nu*, Plon, 2016, 320 p.

DUMONT G., *La citoyenneté administrative*, Thèse pour le doctorat en droit, Université Panthéon-Assas (Paris II), 2002, 750 p.

EYNARD J., E*ssai sur la notion de données à caractère personnel*, thèse, Toulouse I, 2011, 444 p.

FABRE-MAGNAN M., *De l'obligation d'information dans les contrats*, thèse, LGDJ, Bibliothèque de droit privé, Tome 221, 1992, 596 p.

FOUCAULT M., *Surveiller et punir*, Gallimard, 20 février 1975, 352 p.

FOULQUIER N., *Les droits publics subjectifs des administrés*, thèse, Dalloz, Nouvelle Bibliothèque de Thèses, volume n° 25, 2003, 805 p.

GADENNE E., *Le guide pratique du Quantified Self, Mieux gérer sa vie, sa santé, sa productivité*, Editions fyp, 2012, 224 p.

GATES B., *La route du futur*, Pocket, 2 janvier 1997, 332 p.

ESKENAZY D., *Le dispositif médical à la recherche d'un nouveau cadre juridique*, Thèse de doctorat de l'Université Lille 2 Droit et santé, Présentée et soutenue publiquement le 30 novembre 2016, p. 30.

FERAL-SCHUHL C., *Le droit à l'épreuve de l'Internet*, Praxis Dalloz, Dalloz, 2018, 1400 p.

FOUCAULT M., *Sécurité, Territoire, Population*, Le Seuil, 1 octobre 2004, 448 p.

GITELMAN L., *Raw Data is an Oxymoron*, The MIT Press, 2013, p. 4.

GOODMAN M., *Future Crimes*, Double Day, 2015, 429 p.

GREENWALD G., *No Place to Hide, Edward Snowden, the NSA and the Surveillance State*, Penguin Books, 2014, 185 p.

GUTWIRTH S., POULLET Y., DE HERT P., *Data Protection in a Profiled World*, Springer, 2010, p. 124.

HAAS G., *Le RGPD expliqué à mon boss*, Editions Kawa, décembre 2017, p. 123.

HILDEBRANDT M., GUTWIRTH S., *Profiling the European Citizen : Cross-Disciplinary Perspectives*, Springer, 2008, p. 17.

HOCHMANN T., REINHARDT J., *L'effet horizontal des droits fondamentaux*, Pedone, 2018, 216 p.

HONDIUS F., *Emerging Data Protection in Europe*, Amsterdam : North-Holland Publishing Company, 282 p.

ITEANU O., *Quand le digital défie l'Etat de droit*, Editions Eyrolles, septembre 2016, p. 15.

KAYSER P., *La protection de la vie privée*, PUAM, 3e éd., 1995, 457 p.

KELLMEREIT D., OBODOVSKI D., *The Silent Intelligence, the Internet of Things*, DND Ventures, 2013, p. 14.

KLITOU D., *Privacy Invading Technologies and Privacy by Design, Safeguarding Privacy, Liberty and security in the 21st century, Information Technology and Law Series*, Springer, 2014, p. 173.

KUNER C., *European Data Protection Law, Corporate Compliance and Regulation*, Oxford University Press, 2007, p. 121.

LANIER J., *Who Owns the Future ?*, Simon & Schuster, New York, , 2013, 448 p.

LE CLAINCHE J., *L'adaptation du droit des données à caractère personnel aux communications électroniques*, thèse, Montpellier I, 2008, 642 p.

LESAULNIER F., L'information nominative, thèse, Paris II, 2005, 582 p.

LESSIG L., *Code and Other Laws of Cyberspace*, Basic Books, 2006, 424 p.

LEVALLOIS-BARTH C., *La protection européenne des données à caractère personnel et de la vie privée dans le contexte des réseaux et services de communications électroniques*, 2 volumes, thèse, Rennes I, 2003, 964 p.

LIVET P., *L'autorisation administrative préalable et les libertés publiques*, thèse, LGDJ, Bibliothèque de droit public, Tome CXVII, 1974, 334 p.

LYON D., *Surveillance after Snowden*, Polity Press, Octobre 2015, p. 120.

MAETZ O., *Les droits fondamentaux des personnes publiques*, Fondation Varenne, Collection des thèses, Volume 51, 2011, 442 p.

MARTIN L., *Le secret de la vie privée*, Sirey, 1959, 256 p.

MAYER-SCHÖNBERGER V., CUKIER K., *Big Data, A Revolution That Will Transform How We Live, Work and Think*, John Murray, 2013, p. 19.

MOROZOV E., *The Dark Side of Internet Freedom, The Net Delusion*, Public Affairs, 2011, 431 p.

MOROZOV E., *To Save Everything, Click Here, The Folly of Technological Solutionism*, Public Affairs, 2013, 344 p.

MARLAC-NEGRIER C., *La protection des données nominatives informatiques en matière de recherche médicale*, 2 volumes, thèse, PUAM, 2001, 773 p.

MAROT P.-Y., *Les données et informations à caractère personnel. Essai sur la notion et ses fonctions*, thèse, Nantes, 2007, 666 p.

MATTATIA F., *La protection des données à caractère personnel face aux usages illicites, déloyaux et frauduleux*, thèse, Paris X, 2010.

NEMRI M., *Demain, l'Internet des objets*, Commissariat général à la stratégie et à la prospective, France Stratégie, Note d'Analyse, janvier 2015, n°22, p. 3.

NEFF G., NAFUS D., *Self-Tracking*, The MIT Press Essential Knowledge series, The MIT Press, June 2016, 246 p.

NISSEMBAUM H., *Privacy in Context, Technology, Policy and the Integrity of Social Life*, Stanford University Press, 2010, 305 p.

OCHOA N., *Le droit des données personnelles, une police administrative spéciale*, Thèse pour le doctorat en droit présentée et soutenue publiquement le 8 décembre 2014, Université Paris-I Panthéon-Sorbonne, p. 11.

PASQUALE F., *Black Box Society : les algorithmes secrets qui contrôlent l'économie et l'information*, éditions fyp, 2015, 320 p.

PELLEGRINI F., CANEVET S., *Droit des logiciels. Logiciels privatifs et logiciels libres*, PUF, 20 novembre 2013, 616 p.

PERRAY R., JurisClasseur Administratif, Fascicule 274-10 : Informatique. – Données à caractère personnel. – Introduction générale et champ d'application de la loi « Informatique et libertés », 30 juillet 2014, mise à jour du 31 mai 2015.

PERROUD T., *La fonction contentieuse des autorités de régulation en France et au Royaume-Uni*, Thèse pour obtenir le grade de docteur en droit, Université Panthéon-Sorbonne (Paris I), 2011, 1208 p.

PICHARD M., *Le droit à*, thèse, Economica, 2006, 566 p.

PIETTE-COUDOL T., *Les objets connectés, Sécurité juridique et technique*, Lexis Nexis, 2015, 130 p.

PORTEAU-AZOULAI S., *Le pouvoir réglementaire de la Commission nationale de l'informatique et des libertés*, thèse, Paris II, 1993, 504 p.

QUEMENER M., FERRY J., *Cybercriminalité, défi mondial*, Economica, 2ème éd., 2009, 308 p.

RANOUIL V., *L'Autonomie de la Volonté : Naissance et Evolution d'un Concept*, PUF, 1980, 165 p.

RICOEUR P., *La mémoire, l'histoire, l'oubli*, Paris, Seuil, 2000, 736 p.

REY B., *La vie privée à l'ère du numérique*, Lavoisier, 2012, 304 p.

ROQUES-BONNET M.-C., *La Constitution et l'Internet*, thèse, Toulouse I, 2008, 785 p.

ROQUES-BONNET M.-C., *Le droit peut-il ignorer la révolution numérique ?*, Michalon, 4 novembre 2010, 606 p.

ROUSSILLON H., *Liberté Personnelle : une Autre Conception de la Liberté ?*, Presses de l'Université des Sciences Sociales de Toulouse, 1 juin 2006, 159 p.

ROUX A., *La protection de la vie privée dans les rapports entre l'État et les particuliers*, thèse, Economica, 1983, 279 p.

SAINT-PAU J.-C, *L'anonymat et le droit*, 2 volumes, thèse, Bordeaux IV, 1998, 893 p.

SCHNEIER B., *Data and Goliath*, W.W Norton & Company, p. 29.

SCHWARTZ M.-P., SOLOVE J.-D., *Information Privacy Law*, 5e éd., Wolters Kluwer, p. 1134.

SÉE A., *La régulation du marché en droit administratif. Étude critique*, thèse, Strasbourg, 2010, 794 p.

SOLOV J.-D., *The Digital Person : Technology and Privacy in the Information Age*, New York University Press, 2006, 283 p.

SOLOV J.-D., *Nothing to Hide : The False Tradeoff between Privacy and Security*, Yale University Press, 2011, 245 p.

SUPIOT A., *La Gouvernance par les nombres, Cours au collège de France*, 2012-2014, Fayard, 2015, p. 216.

TÜRK A., *Le droit public français face au progrès technologique*, 2 volumes, thèse, Lille II, 1984, 317 p.

TÜRK A., *La vie privée en péril. Des citoyens sous contrôle*, Odile Jacob, Avril 2011, 272 p.

TOPOL E., *The Creative destruction of medicine : How the digital revolution will create better health care*, Basic Books, 2012, 336 p.

UNTERSINGER M., *Anonymat sur internet : Protéger sa vie privée*, Editions Eyrolles, 29 octobre 2014. 264 p.

VERDUN F., *La gestion des risques juridiques*, Editions d'organisation, Eyrolles, 2006, p. 11.

VITALIS A., *Informatique, pouvoir et libertés publiques*, thèse, Rennes, 1979, 842 p.

WATSON S.-M, *Living with Data : Personal Data Uses of the Quantified-Self*, Oxford Internet Institute Masters Thesis, 2013, 47 p.

WESTIN A.-F, SOLOVE D.-J, *Privacy and freedom*, Athenum, New York, 1967, 500 p.

III. ARTICLES DE DOCTRINE, CONTRIBUTIONS, NOTES DE JURISPRUDENCE ET CONCLUSIONS

ACKERMAN L., « Mobile health and fitness applications and information privacy », *Privacy Rights Clearinghouse*, San Diego, 2013, p. 2.

ADAM A., « L'échange de données à caractère personnel entre l'Union européenne et les États-Unis, Entre souci de protection et volonté de coopération », *RTDE*, n° 42 (3), juillet-septembre, 2006, pp. 411-437.

ADELE P.-A., DESMOULIN-CANSELIER S., « Droit des dispositifs médicaux : vers une réforme ou un simple réaménagement ? », *RDSS*, 2016, p. 930.

AGOSTI P., CAPRIOLI E., « La confiance dans l'économie numérique (commentaires de certains aspects de la loi pour la confiance dans l'économie numérique) », *LPA*, 3 juin, 2005, n° 110, p. 4.

AÏDAN G., « De la démocratie administrative à la démocratie sanitaire dans le secteur public de la santé », *RFAP*, 2011, n° 137-138, pp. 139-153.

AILINCAI M., « Espoirs et inquiétudes autour de la révision du cadre juridique général de l'Union européenne sur la protection des données à caractère personnel », *Revue de l'Union Européenne*, 2014, p. 170.

ANCEL P., « La protection des données personnelles : aspects de droit privé français », *RICD*, 1987, vol. 39, n°3, p. 611.

ANCIAUX A., FARCHY J., « Données personnelles et droit de propriété : quatre chantiers et un enterrement », *Revue internationale de droit économique*, 2015, n° 3, p. 307-331.

ANDRIEU B., « Traquer son bien-être et propriété des données : quel droit des sportifs 3.0 sur leur corps vivant ? », *JS*, 2016, n°162, p. 36.

APOLLIS B., « Vers une transformation financière du système de santé ? », *RDSS*, 2019, p. 35.

ASHTON K., « That 'Internet of Things' Thing », *RFID Journal*, June 22, 2009, p. 97-114.

AUBY J.-B., « Le droit administratif face aux défis du numérique », *AJDA*, 2018, p. 835.

AUGAGNEUR L.-M., « Vers des nouveaux paradigmes du droit dans l'économie numérique », *RTD Com*., 2015, p.455.

AUGAGNEUR L.-M., « Les clauses abusives des conditions de Google », *AJ Contrat*, 2019, p. 175.

ASHTON K., « That 'Internet of Things' thing : In the real world things matter more than ideas », *RFID Journal*, June 22, 2009.

ASTAY A., « Internet : le Conseil national du numérique (re)devient une réalité », *Dalloz Actualité*, 4 mai 2011.

ASTAIX A., « Réfléchir aux agences, c'est réfléchir à l'État », *Dalloz Actualité*, 17 septembre 2012.

BACHERT-PERETTI A., « La protection constitutionnelle des données personnelles : les limites de l'office du Conseil constitutionnel face à la révolution numérique », *Revue française de Droit constitutionnel*, 2019/2, n° 118, p. 261 à 284.

BADINTER R., « Le Droit au Respect de la Vie privée », *JCP G*, 1968, I, 2136, n°22.

BALLET P., « Où en est la procédure d'agrément des hébergeurs de données de santé à caractère personnel ? », *Gaz. Pal.*, 19 avril 2007, n° 109, p. 20.

BARBIER-CHASTAING F., « Garantir la sécurité des données et mieux prendre en compte la cybercriminalité dans une logique de responsabilisation pour les entreprises », *Dalloz IP/IT*, 2019, p. 217.

BARDIN M., « Le droit d'accès à internet : entre « choix de société » et protection des droits existants », *RLDI*, n° 91, mars 2013, pp. 79-87.

BARNES S.-B., « A Privacy Paradox : Social Networking in the United States », *First Monday*, April 2006.

BEER-GABEL J., « Le contrôle de l'administration par la Commission Nationale de l'Informatique et des Libertés », *RDP*, 1980, pp. 1043-1070.

BELLANGER P., « De la souveraineté numérique », *Le Débat*, vol. 170, no. 3, 2012, pp. 149-159.

BELLANOVA R., DE HERT P., « Le cas S. et Marper et les données personnelles : l'horloge de la stigmatisation stoppée par un arrêt européen », *Cultures & Conflits*, n° 76, hiver 2009, pp. 101-114.

BELLEIL A., « La régulation économique des données personnelles ? », *Légicom*, n° 42, 2009/4, pp. 143-151.

BENOÎT-ROHMER F., « Chronique Union européenne et Droits fondamentaux – L'adoption de mesures visant à renforcer la protection des données personnelles », *RTD eur.*, 2017, p. 355.

BENSAMOU A., ZOLYNSKI C., « Big data et privacy : comment concilier nouveaux modèles d'affaires et droits des utilisateurs », *Les Petites Affiches*, 18 août 2014, n° 164, p. 8.

BERGÉ J.-S., « La protection du droit d'auteur et des données à caractère personnel : étude d'un phénomène de communautarisation du droit des conflits de lois », *in*

FUCHS A., MUIR-WATT H. et PATAUT E. (dir.), *Les conflits de loi et le système juridique communautaire*, Dalloz, 2004, pp. 225-241.

BERNAL P., « Web 2.5: the symbiotic web », *International review of Law, Computers & Technology*, n° 24/1, 2010, p. 25 à 37.

BERTHET C., ZOLYNSKI C., ANCIAUX N., PUCHERAL P., « Contenus numériques, récupération des données et empouvoirement du consommateur », Dalloz IP/IT, 2017, p. 29.

BERTHIER T., « Projections algorithmiques et cyberespace », *Revue internationale d'intelligence économique*, 5.2, 2013, p. 179-195.

BESSIERE T., « Loi informatique et libertés : la CNIL veille », *JS*, 2011, n°111, p. 20.

BESSIERE T., « La collecte de données personnelles : un cadre précis à respecter », *JS*, 2011, n°111, p. 22.

BISMUTH Y., « Les clauses-types dans les contrats informatiques : le surgelé contractuel », *Cahiers de droit de l'entreprise*, n° 4, juillet 2008, 39, pp. 44-47.

BLACK-GONNET JONASON P., « Vers une meilleure adaptation du droit de la protection des données personnelles à la réalité informationnelle », *AJDA*, 2008, p. 2105.

BLANCK A., « GDPR et sous-traitance : un nouveau devoir de conseil ? », *Dalloz IP/IT*, 2017, p. 36.

BLOUSTEIN E.-J., « Privacy as an Aspect of Human Dignity », *New York University Law Review*,1964, n° 39, DeCew, 1997 pp. 962-1007.

BLOUD-REY C., « Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ? », *Recueil Dalloz*, 2013, p. 2795.

BOIZARD M., « La valorisation des données numériques par la protection juridique des algorithmes », *Dalloz IP/IT*, 2018, p. 99.

BOSSI J., « Comment organiser aujourd'hui en France la protection des données de santé ? », *RDSS*, 2010, p. 208.

BOUCOBZA I., « La « co-administration » dans la production des normes juridiques communautaires », *DA*, décembre 2004, pp. 7-13.

BOURCIER D., « Données sensibles et risque informatique – De l'intimité menacée à l'intimité virtuelle », *in* CURAPP, « Questions sensibles », *PUF*, 1998, pp. 39-58.

BRAIBANT G., « L'informatique dans l'administration », *RISA*, 1968, pp. 341-346.

BRAIBANT G., « Perspectives et problèmes du développement de l'informatique dans l'administration publique au cours de la prochaine décennie », *RISA*, 1971, pp. 201-211.

BRAIBANT G., « La protection des droits individuels au regard du développement de l'informatique », *RIDC*, 1971, n°4, pp. 793-817.

BRAIBANT G., « Droit d'accès et droit à l'information », *in* Service public et libertés, Mélanges offerts au Professeur Robert-Édouard CHARLIER, Éditions de l'université et de l'enseignement moderne, 1981, pp. 703-710.

BRAUD C., « La notion d' « agence » en France : réalité juridique ou mode administrative ?, *Les Petites Affiches*, 30 août 1995, n° 104, p. 4.

BROSSET E., « Le droit à l'épreuve de la e-santé : quelle connexion du droit de l'Union européenne ? », *Revue de Droit Sanitaire et Social*, Dalloz, 2016, p. 869.

BRUGUIERE J.-M., Le « droit à » l'oubli numérique, un droit à oublier, Recueil Dalloz, 2014, p. 299.

BRUNAUX G., « Cloud computing, protection des données : et si la solution résidait dans le droit des contrats spéciaux ? », *Recueil Dalloz*, 2013, p. 1158.

BULLICH V., CLAVIER V., « Production des données, « Production de la société ». Les Big Data et algorithmes au regard des Sciences de l'information et de la

communication », *Les Enjeux de l'Information et de la Communication*, Lavoisier, 2018, vol. 2, p. 5 à 14.

BURKERT H., « Progrès technologique, protection de la vie privée et responsabilité politique », *RFAP*, n° 89, janvier-mars 1999, pp. 119-129.

BURTON C. et PROUST O., « Le conflit de droit entre les règles américaines de e-discovery et le droit européen de la protection des données à caractère personnel... entre le marteau et l'enclume », *RLDI*, 2009, n° 46, pp. 79-84.

BYK C., « Biométrie et Constitution : est-il déjà trop tard pour les libertés publiques ? », *JCP*, n° 25, 18 juin 2008, pp. 19-22.

CADIO P., LIVENAIS T., « Photographie du champ territorial du règlement données personnelles : de nouveaux opérateurs concernés ? », *Dalloz IP/IT*, 2016, p. 347.

CADOUX L., TABATONI P., « Les défis d'Internet à la protection de la vie privée : institutions, marchés et techniques en Europe et aux États-Unis », in TABATONI P. (dir.), La protection de la vie privée dans la société d'information, tome 1, *PUF*, cahier des sciences morales et politiques, 2000, pp. 15-36.

CAPRIOLI E., « Loi du 6 août 2004. Commerce à distance sur l'Internet et protection des données à caractère personnel », *CCE*, février 2005, pp. 24-39.

CARDON D., « L'identité comme stratégie relationnelle », *Hermès, La Revue*, vol. 53, no. 1, 2009, p. 61-66.

CARMINATI J.-P., « Les non-dénonciations de la CNIL au parquet. Une pratique contra legem aux effets pervers », *Expertises*, février / mars 1995, p. 67 et 106.

CARRERA-MARISCAL A., « Le CIL : modèle type du futur délégué à la protection des données ? », *Dalloz IP/IT*, 2018, p. 233.

CASTETS-RENARD C., « L'invalidation de la directive n° 2006/24/CE par la CJUE : une onde de choc en faveur de la protection des données personnelles », *Rec. Dalloz*, 26 juin 2014, n° 23, pp. 1355-1359.

CASTETS-RENARD C., « Le Privacy Shield », *Dalloz IP/IT*, 2016, p. 113.

CASTETS-RENARD C., « L'adoption du Privacy Shield sur le transfert de données personnelles », *Recueil Dalloz*, 2016, p. 1696.

CASTETS-RENARD C., « Adoption du Privacy Shield : des raisons de douter de la solidité de cet accord », *Dalloz IP/IT*, 2016, p. 444.

CASTETS-RENARD C., NDIOR V., RASS-MASSON L., « Le marché unique numérique : quelles réalités matérielles et conceptuelles ? », *Recueil Dalloz*, 2019, p. 956.

CAVOUKIAN A., « Privacy by Design, The 7 Foundational Principles », *Information and Privacy Commissioner of Ontario*, January 2011.

CAVOUKIAN A., « Privacy by design [leading edge] », *IEEE Technology and Society Magazine*, vol. 31, n°4, 2012, p. 18 à 19.

CAYLA J.-S., « Le principe de précaution, fondement de la sécurité sanitaire », *RDSS*, 1998, p. 491.

CAZENEUVE J., « La cybercriminalité : l'émergence d'un nouveau risque », *AJ pénal*, 2012, p. 268.

CECERE G., LE GUEL F., ROCHELANDET F., « Les modèles d'affaires numériques sont-ils trop indiscrets ? Une analyse empirique », *Réseaux*, n° 189, 2015, p. 77 à 101.

CHAFIOL F., BARBET-MASSIN A., « La blockchain à l'heure de l'entrée en application du règlement général sur la protection des données », *Dalloz IP/IT*, 2017, p. 637.

CHAMPEIL-DESPLATS V., « La notion de droit « fondamental » et le droit constitutionnel français », *Rec. Dalloz*, 1995, pp. 323-329.

CHAUVAUX D., GIRARDOT X.-T., « Régime de la déclaration préalable des traitements informatisés d'informations nominatives », *AJDA*, 1997, p. 156.

CHARPENTIER P.-Y., « La gestion du risque : de l'approche juridique à l'ébauche d'une méthodologie managériale », *Management & Avenir*, vol. 74, no. 8, 2014, p. 191 à 209.

CHEVALLIER J., « COB, CNIL, CNCL et Cie : la « philosophie » des autorités administratives indépendantes », *Regards sur l'actualité*, n° 146, décembre 1988, pp. 13-28.

CHEVALLIER J., « De quelques usages du concept de régulation », *in* MIAILLE M. (dir.), *La régulation entre droit et politique*, L'Harmattan, 1995, pp. 71-93.

CHEVALLIER J., « Mondialisation du droit ou droit de la mondialisation », *in* MORAND C.-A. (dir.), *Le droit saisi par la mondialisation*, Bruylant, 2001, pp. 37-61.

CHEVALLIER J., « Contractualisation et régulation », *in* CHASSAGNARD-PINET S. et HIEZ D. (dir.), *La contractualisation de la production normative*, Dalloz, 2008, pp. 83-93.

CLAUDEL E., « Action de groupe et autres dispositions concurrence de la loi consommation : un dispositif singulier », *RTD com.*, 2014, p. 339.

CLEMENT-FONTAINE M., « L'union du droit à la protection des données à caractère personnel et du droit à la vie privée », *LEGICOM*, vol. 59, no. 2, 2017, p. 61.

CLUZEL-METAYER L., « Les téléservices publics face au droit à la confidentialité des données », *RFAP*, 2013/2, n° 146, pp. 405-418.

CLUZEL-METAYER L., « Les limites de l'Open Data », *AJDA*, 2016, p. 102.

CLUZEL-METAYER L., « La loi pour une République numérique : l'écosystème de la donnée saisi par le droit », *AJDA*, 2017, p. 340.

CLUZEL-METAYER L., DEBAETS E., « Le droit de la protection des données personnelles : la loi du 20 juin 2018 », *RFDA*, 2018, p. 1101.

COHEN D., « Ampleur et qualités du consentement donné par clic de souris », *Les Petites Affiches*, numéro 164, 2015, p. 3.

COHEN-TANUGI L., « L'émergence de la notion de régulation », *LPA*, 10 juillet 1998, p.4.

COLLET M., « La réforme de la CNIL ou les ruses de l'État « post-moderne » », in *Annales de la régulation*, Volume 1 (2006), LGDJ, pp. 127-150.

CONFINO F., « Le « choc » du numérique sur la gouvernance, les enjeux et les stratégies de communication des collectivités locales », *L'Actualité Juridique : Collectivités Territoriales*, 2014, p.595.

COSTAZ C., « Le droit à l'oubli », *La Gazette du Palais*, 27 juillet 1995, p. 961.

CORBY J.-M., « The case for privacy », *Information Systems Security*, 2002, vol. 11, n° 2, p. 9.

CRAIN M., « The limits of transparency : Data brokers and commodification », *New Media & Society*, Vol 20, Issue 1, July 2016, pp. 88 – 104.

CRENN J.-P., « Les objets connectés décryptés pour les juristes », *Dalloz IP/IT*, 2016, p. 389.

CRUCIS H.-M., « Le Parlement face aux sciences et technologies », AJDA, 1991, pp. 448-455.

CYTERMANN L., « La loi Informatique et Libertés est-elle dépassée ? », *RFDA*, 2015, p. 99.

DAMON J., « Révolution numérique : sécurité sociale 2.0 et médecine « 5P » », *RDSS*, 2017, p. 925.

DAOUD E., PERONNE G., « Cyberattaques : la lutte s'intensifie », *AJ pénal*, 2015, p. 396.

DAOUD E., PLENACOSTE F., « Cybersécurité et Objets Connectés », *Dalloz IP/IT*, 2016, p. 409.

DARY M., BENAISSA L., « Privacy by Design : un principe de protection séduisant mais complexe à mettre en œuvre », *Dalloz IP/IT*, 2016, p. 476.

DEBIES E., « L'ouverture et la réutilisation des données de santé : panorama et enjeux », *RDSS*, 2016, p. 697.

DEBET A., « Informatique et libertés : faut-il aujourd'hui réviser la directive 95/46/CE relative à la protection des données personnelles ? », *Recueil Dalloz*, 2011, p. 1034.

DEBET A., « Programme Prism : les citoyens européens sur écoute », *Recueil Dalloz*, 2013, p. 1736.

DEBET A., « La Commission des clauses abusives et la protection des données personnelles sur les réseaux sociaux : une incursion hésitante dans un territoire inconnu », *Revue des contrats*, septembre 2015, n°3, p. 496.

DEBET A., « Arrêt Weltimmo : un nouvel élargissement par la CJUE de la notion d'établissement », *Communication Commerce électronique*, décembre 2015, n°12.

DEBET A., « La protection des données personnelles, point de vue du droit privée », *Revue du Droit public*, n°1, 2016, p. 17.

DELMAS-MARTY M., « La mondialisation du droit : chances et risques », *Recueil Dalloz*, 1999, p. 43.

DE FILIPPI P., MC CARTHY S., « Cloud computing centralization and data sovereignty », *European Journal of Law & Technology*, Vol. 3, No 2, 2012.

DERIEUX E., « Neutralité : liberté ou surveillance. Fondements et éléments du droit de l'internet », *RLDI*, n° 74, août-septembre 2011, pp. 85-96.

DERIEUX E., « Vie privée et données personnelles – Droit à la protection et « droit à l'oubli » face à la liberté d'expression », *Les Nouveaux Cahiers du Conseil constitutionnel*, 2015/3, n°48, p. 21 à 33.

DELISLE E., « Le nouveau rôle de la CNIL », *JS*, n° 196, 2019, p. 32.

DELTORN J.-M., « La protection des données personnelles face aux algorithmes prédictifs », *RDLF*, 2017, chron. n°12.

DEROUDILLE A., « Le secret professionnel dans le règlement général sur la protection des données », *RFDA*, 2018, p. 1112.

DEROUDILLE A., FATAH F., « L'extraterritorialité du RGPD dans le contexte du « Cloud Act » », Rev. UE, 2019, p. 442.

DE SCHUTTER O., « La vie privée entre droit de la personnalité et liberté », *RTDH*, 1999, pp. 827-863.

DE SCHUTTER O., « Vie privée et protection de l'individu vis-à-vis des traitements de données à caractère personnel », note sous CEDH, 4 mai 2000, Rotaru c. la Roumanie, *RTDH*, 2001, pp. 137-183.

DESFORGES A., « Les représentations du cyberespace : un outil géopolitique », *Hérodote*, vol. 152-153, no. 1, 2014, pp. 67-81.

DESGENS-PASANAU G., « Informatique et libertés, une équation à plusieurs inconnues », in GIROT Jean-Luc (dir.), *Le harcèlement numérique*, Dalloz, 2005, pp. 75-113.

DESGENS-PASANAU G., « RGPD : entre incertitudes et occasions manquées », *Dalloz IP/IT*, 2016, p. 335.

DE SILVA I., « Données, algorithmes et transparence des plateformes. Quels impacts sur la concurrence ? Quels enjeux pour la régulation ? (Retour sur les rendez-vous de l'Autorité de la concurrence du 24 nov. 2017) », *Dalloz IP/IT*, 2018, p. 8.

DEVILLIER N., « Jouer dans le « bac à sable » réglementaire pour réguler l'innovation disruptive : le cas de la technologie de la chaîne de blocs », *RTD com*, 2017, p. 1037.

DOUAY Sophie, « L'identité personnelle dans la civilisation de réseaux », *Rec. Dalloz*, 2007, n° 37, p. 2623.

DOUVILLE T., « Données non personnelles (libre flux) : publication d'un règlement européen », *Recueil Dalloz*, 2019, p. 10.

DREYER E., « Le respect de la vie privée, objet d'un droit fondamental », *CCE*, mai 2005, n° 5, Étude n° 18, pp. 21-26.

DREYER E., « La fonction des droits fondamentaux dans l'ordre juridique », *Rec. Dalloz*, 2006, n°11, pp. 748-75.

DUBOIS L, GAULLIER F., « Publicité ciblée en ligne, protection des données à caractère personnel et ePrivacy : un ménage à trois délicat », *LEGICOM*, vol. 59, no. 2, 2017, p. 69.

DUCLERCQ J.-B., « Le droit public à l'ère des algorithmes », *Revue du Droit Public*, n° 5, 2017, p. 1402.

DUFOUR O., « L'exercice du pouvoir de sanction est une révolution culturelle pour la CNIL », *Les Petites Affiches*, n° 195, 29 septembre 2004, p. 3.

DUFOUR O., « Et si le droit souple était l'avenir du droit dur ? », *Les Petites Affiches*, n° 221, 5 novembre 2013, p. 4.

DUMORTIER F. et POULLET Y., « La protection des données à caractère personnel dans le contexte de la construction en piliers de l'Union européenne », *RLDI*, juillet 2007, n° 29, pp. 76-86.

EMORINE A., « Les données personnelles des français protégées par les autorités irlandaises, allemandes et luxembourgeoises : l'Europe des droits numériques en marche ... sans la Commission », *Les Petites Affiches*, n°245, 9 décembre 2015, p. 7.

EON F., « L'accélération du numérique en santé : enjeux et conditions de son succès », *RDSS*, 2019, p. 55.

EYNARD J., « Pokémon GO et le droit : quel cadre juridique pour la réalité augmentée ? », *Les Petites Affiches*, 18 août 2017, n°164-165, p. 5.

FALAISE M., « Bien-être animal et abattage : la nouvelle donne européenne », *Revue de l'Union Européenne*, 2012, p. 331.

FALQUE-PIERROTIN I., « La Constitution et l'Internet », *Les Nouveaux Cahiers du Conseil Constitutionnel*, 2012/3, n° 36, p. 31 à 44.

FALQUE-PIERROTIN I., « Le droit souple vu de la CNIL : un droit relais nécessaire à la crédibilité de la régulation des données personnelles », in *Le droit souple*, EDCE, 2013, pp. 239-255.

FALQUE-PIERROTIN I., « La CNIL face à l'économie de la donnée », *AJCA*, 2016, p. 175.

FARSHIAN M., « Quand la réalité de la surveillance massive tend à dépasser la fiction orwellienne », *La Revue des droits de l'homme*, Revue du Centre de recherches et d'études sur les droits fondamentaux, 2015.

FAUVET J., « La protection des données personnelles », *RIDC*, Vol. 39 n°3, Juillet-septembre 1987, pp. 551-556.

FAUVET J., « La commission nationale de l'informatique et des libertés, vingt ans après... », *in Libertés*, Mélanges Jacques ROBERT, Monchrestien, 1998, pp. 111-123.

FAVREAU B., « La protection des données à caractère personnel », *IDHAE*, 2009, p. 7.

FERREOL G., « Qu'entend-on par bien-être ? Un éclairage socio-économique », *JS*, 2015, n°151, p. 31.

FLEURIOT C., « L'action de groupe s'ouvre à de nouveaux domaines », *Dalloz Actualité*, 22 novembre 2016.

FONTAINE M., JUILLET S., FROGER D., « La donnée numérique : l'or noir du XXIème siècle ? », *Les Petites Affiches*, 8 septembre 2017, n°179-180, p. 90.

FOREST D., « Pouvoirs de sanction de la CNIL : le réveil soudain de la belle endormie », *Recueil Dalloz*, 2007, p. 94.

FOREST D., « La régulation des algorithmes, entre éthique et droit », *Lamy Droit de l'Immatériel*, n° 137, 2017, pp. 38-42.

FOREST D., « Conservation des données de connexion et métadonnées : un nouveau coup de semonce à la surveillance de masse en Europe », *Dalloz IP/IT*, 2017, p. 230.

FOURETS F., « La protection des données, ou le symbole d'une démocratie nouvelle. Le contrôle de la CNIL », *Informations sociales*, vol. 126, no. 6, 2005, pp. 94-103.

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.

FRANCILLON J., « Cyberdélinquance. Piratage informatique. Maintien frauduleux dans un STAD. Vol de données », *RSC*, 2015, p. 887.

FRANCILLON J., « De quelques atteintes à la réputation des personnes : e-réputation, cyber-harcèlement, usurpation d'identité numérique, menace de révélation diffamatoire... », *RSC*, 2016, p. 544.

FRAYSSINET J., « L'informatique et le secret des fichiers », *RA*, 1977, pp.175-185.

FRAYSSINET J., « L'utilité et les fonctions d'une formulation d'objectifs : l'exemple de la loi du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés », *RRJ*, 1989-4, pp. 903-918.

FRAYSSINET J., « Le conseil constitutionnel et la loi relative à l'informatique, aux fichiers et aux libertés (n° 92-316 DC, 20 janvier 1993) », *RFDC*, 1993, n° 14, pp. 395-405.

FRAYSSINET J., « Le transfert et la protection des données personnelles en provenance de l'Union européenne vers les États-Unis : l'accord dit « sphère de sécurité » ou safe harbour », *CCE*, 2001, n°3, pp. 10-14.

FRAYSSINET J., « La loi relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004 : continuité et/ou rupture ? », *RLDI*, 2005, n°9, pp. 50-55.

FRAYSSINET J., « Trente ans après, la loi « Informatique et libertés » se cherche encore », *RLDI*, janvier 2008, n° 34, pp. 69-73.

FRAYSSINET Jean, « Le projet de loi relatif à la protection des personnes physiques à l'égard des traitements des données à caractère personnel : constantes et nouveautés », *CCE*, janvier 2002, pp. 11-15.

FRAYSSINET J., KAYSER P., « La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et le décret du 17 juillet 1978 », *RDP*, 1979, pp. 629-691.

FRAYSSINET J., « La régulation de la protection des données personnelles », *Légicom*, n° 42, 2009/4, pp. 5-9.

FRAYSSINET J., « La régulation du respect de la loi informatique, fichiers et libertés par le droit pénal : une épée en bois », *Légicom*, n° 42, 2009/4, pp. 23-3.

FRIED C., « Privacy », *The Yale Law Journal*, Vol. 77, n°3, January 1968, pp. 475-493.

FRISON-ROCHE M.-A., « Le droit de la régulation », *Rec. Dalloz*, 2001, pp. 610-616.

FRISON-ROCHE M.-A., « Les nouveaux champs de la régulation », *RFAP*, n° 109, 2004, pp. 53-63.

FROMONT M., « Jurisprudence constitutionnelle de la République fédérale d'Allemagne (2008) », *Revue du Droit public*, novembre 2009, n°6, p. 1721.

GALLOUX J.-C., « Ebauche d'une définition juridique de l'information », *Recueil Dalloz*, 1994, p. 229.

GAMBARDELLA S., « Une lecture de la jurisprudence de la Cour européenne des droits de l'Homme relative aux données de santé », *RDSS*, 2016, p. 271.

GAUDEMET M., PERRAY R., « « Scoring » et protection des données personnelles : un nouveau régime à l'efficacité incertaine », *LPA*, 30 mai 2006, n° 107, pp. 8-10.

GAZIER F., CANNAC Y., « Étude sur les autorités administratives indépendantes », *EDCE*, 1983-1984, pp. 13-77.

GEFFRAY E., « La protection des données personnelles, élément clé à l'ère du numérique », *Légipresse*, oct. 2014, n° 320.

GEFFRAY E., « Droits fondamentaux et innovation : quelle régulation à l'ère numérique ? », *Les nouveaux Cahiers du Conseil constitutionnel*, n°52, juin 2016, p. 7.

GENDREAU A., « La dématérialisation du dépôt : l'exemple du contrat de cloud computing », *AJ contrat*, 2016, p. 519.

GEORGOPOULOS T., « Libertés fondamentales communautaires et droits fondamentaux européens : le conflit n'aura pas lieu », *LPA*, 8 janvier 2004, n° 6, pp. 6-14.

GHEORGHE-BADESCU I., « Le nouveau règlement général sur la protection des données », *Revue de l'Union européenne*, Dalloz, 2016, p. 466.

GILBERT F., « La FTC américaine propose des principes pour encadrer la publicité comportementale sur Internet », *La Gazette du Palais*, 24 avril 2008, n° 115, p. 17.

GIRAUD T., « Les licences Creative Commons, une culture du partage », *JAC*, 2014, n°10, p. 36.

GODEFROY L.-D., « Pour un droit du traitement des données par les algorithmes prédictifs dans le commerce électronique », *Recueil Dalloz*, 2016, p. 438.

GRANJON F., « Du (dé)contrôle de l'exposition de soi sur les sites de réseaux sociaux », *Les Cahiers du numérique*, 2014, Vol. 10, pp. 19-44.

GRIGUER M., « Vers une compatibilité de la loi informatique et libertés avec les lois américaines », *Cahiers de droit de l'entreprise*, mars-avril 2010, n°2, pp. 45-51.

GRUBER A., « Le système français de protection des données personnelles », *LPA*, 4 mai 2007, n°90, pp. 4-13.

GUILLAUME B., « Dispense, déclarations ou autorisation : la nature des données fait la différence », *JA*, 2007, n°357, p. 13.

HAAS G., « La cybercriminalité à la fois côté obscur et face cachée du Big Data », *Dalloz IP/IT*, 2016, p. 21.

HAAS G., DUBARRY A., « Confidentialité et protection des données », *Dalloz IP/IT*, 2017, p. 322.

HAAS G., DUBARRY A., D'AUVERGNE M., RUIMY R., « Enjeux et réalités juridiques des Objets Connectés », *Dalloz IP/IT*, 2016, p. 394.

HAAS G., « Bilan après neuf mois d'application du RGPD », Dalloz IP/IT, 2019, p. 357.

HONDIUS W. F., « Data Law in Europe », *Stanford Journal of International Law*, 1980, pp. 87-111.

HOUSSIN D., « Le secret médical dans les nouvelles pratiques et les nouveaux champs de la médecine », *Recueil Dalloz*, 2009, p. 2619.

JACOMINO F., « Mise en conformité des conditions générales d'utilisation de Facebook : la Commission européenne s'impatiente », *AJ Contrat*, 2018, p. 521.

JACQUÉ J.-P., « La Convention pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel », *AFDI*, 1980, pp. 773-789.

JACQUÉ J.-P., « Protection des données personnelles, Internet et conflits entre droits fondamentaux devant la Cour de justice », *RTDE*, avril-juin 2014, pp. 283-288.

JAULT-SESEKE F., ZOLYNSKI C., « Le règlement 2016/679/UE relatif aux données personnelles », *Recueil Dalloz*, 2016, p. 1874.

KOUBI G., « Les données à caractère personnel, outil des services de renseignement », *JCP A*, 2009, n° 46, pp. 30-34.

LAÏDI Z., « Mondialisation et droit », *Recueil Dalloz*, 2007, p. 2712.

LANERET N., HAMON S., Nathalie Laneret, Solène Hamon, « Quel avenir pour les transferts internationaux ? », *Dalloz IP/IT*, 2018, p. 31.

LANGLET V., « Nom de code : délégué à la protection des données », *Juris Tourisme*, 2018, n°207, p. 29.

LANGE T., « Cloud computing et données personnelles : les clauses à maîtriser », *Dalloz IP/IT*, 2016, p. 459.

LATOUR X., « Le droit communautaire et la protection des données à caractère personnel dans le commerce électronique », *LPA*, 6 février 2004, n° 27, pp. 9-16.

LAVENUE J.-J., « La privacy by design : panacée ou cheval de Troie ? », *Revue de la Recherche Juridique*, Droit Prospectif, 2013-1, pp. 59-73.

LAZARO J.-J., LE METAYER D., « Le consentement au traitement des données personnelles : une perspective comparative sur l'autonomie du sujet », *Revue juridique Thémis de l'Université de Montréal*, voL.48, n°3, 2015, pp. 765-815.

LE BONNIEC N., « Vers une convergence des exigences constitutionnelles et européennes en matière de protection des données personnelles numériques ? », *La Semaine Juridique*, Edition Générale, n° 23, 4 juin 2018, p. 1129.

LHERNOULD J.-P., « Professionnels de santé et assurance maladie dans un espace européen sans frontières », *RDSS* 2010, p. 1004.

LECLERCQ P., « Loi du 6 août 2004. Les transferts internationaux de données personnelles », *CCE*, février 2005, pp. 29-32.

LE CLAINCHE J., « L'évolution du contrôle des interconnexions de fichiers publics », *Légicom*, n° 47, 2011/2, pp. 65-72.

LEPAGE A., « Internet, Territoires et État : le franchissement dématérialisé des frontières », *Revue générale des collectivités territoriales*, numéro spécial, novembre 2002, pp. 47-51.

LEPAGE A., « Consentement et protection des données à caractère personnel », in GIROT Jean-Luc (dir.), *Le harcèlement numérique*, Dalloz, 2005, pp. 227-251.

LEPAGE A., « Droit pénal et internet : la part de la tradition, l'oeuvre de l'innovation », *AJ pénal*, 2005, p. 217.

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 », *Droit pénal*, mars 2005, n° 3, p. 20.

LEPAGE A., « L'article 9 du Code civil peut-il constituer durablement la « matrice » des droits de la personnalité ? », *Gaz. Pal.*, Recueil mai-juin 2007, pp. 1497-1500.

LEQUILLERIER C., « L'« ubérisation » de la santé », *Dalloz IP/IT*, 2017, p. 155.

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.

LESSIG L., « Code is law, On liberty in Cyberspace », *Harvard Magazine*, January - February, 2000.

LE TOURNEAU P., « Pot-pourri (réflexions incongrues autour de l'informatique et de l'internet) », *CCE*, janvier 2004, pp. 11-14.

LETTERON R., « Le droit à l'oubli », *RDP*, mars-avril 1996, n° 2, pp. 385-424.

LONGOBARDI N., « Les autorités administratives indépendantes, laboratoires d'un nouveau droit administratif (suite et fin) », *LPA*, 31 août 1999, n° 173, pp. 10-15.

LOISEAU G., « Typologie des choses hors du commerce », *RTD Civ.*, 2000, p. 47.

LOISEAU G., « La valeur contractuelle des conditions générales d'utilisation des réseaux sociaux », *Communication Commerce électronique*, n°7-8, Juillet 2012.

LU X., QU Z., LI Q., HUI P., « Privacy Information Security Classification for Internet of Things Based on Internet Data », *International Journal of Distributed Sensor* Networks, 2015, vol. 2015.

LUPPI P., « L'unité du pouvoir réglementaire du Premier ministre et son caractère ab initio », *AJDA*, 2007, p. 1643.

LUPTON D., « Quantifying the body : monitoring and measuring health in the age of mHealth technologies », *Critical Public Health*, 2013, n°23, p. 393 à 403.

MAIANI F., « Le cadre réglementaire des traitements de données personnelles effectués au sein de l'Union européenne », *RTD eur.*, 2002, p.283.

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*, 1978, I, 2891.

MAISL H., « La modification du droit sous l'influence de l'informatique, aspects de droit public », *JCP*, 1983, I, 3101.

MAISL H., « Informatique et libertés publiques », in *Émergence du droit de l'informatique*, Actes des deuxièmes entretiens de droit de l'informatique de Nanterre organisés les 11 et 12 mai 1982, Édition des Parques, 1983, pp. 113-123.

MAISL Herbert, « La commercialisation des données administratives », *AJDA*, 1988, pp. 637-642.

MAISL H., « État de la législation française et tendances de la jurisprudence relatives à la protection des données personnelles », *RIDC*, 3-1987, pp. 559-580.

MAISL H., « Les autorités administratives indépendantes : protection des libertés ou régulation sociale ? », *in* COLLIARD C.-A. et TIMSIT G. (dir.), *Les autorités administratives indépendantes*, PUF, 1988, pp. 75-89.

MAISL Herbert, « La loi « informatique et liberté » amputée d'un article », *Droit de l'informatique et des télécoms*, 1988, n° 2, pp. 71-72.

MAISL Herbert, « De l'administration cloisonnée à l'administration en réseau : fin de la vie privée et/ou satisfaction de l'usager ? », in CHATILLON G., DU MARAIS B. (dir.), *L'administration électronique au service des citoyens*, Actes du colloque du Conseil d'État et de l'Université Paris I Panthéon-Sorbonne, Paris, 21 et 22 janvier 2002, Bruylant, 2003, pp. 349-359.

MAISL H., « Etat de la législation française et tendances de la jurisprudence relatives à la protection des données personnelles », *Revue Internationale de Droit comparé*, n°3, 1987, p. 559-580.

MAITROT DE LA MOTTE A., « La réforme de la loi informatique et libertés et le droit au respect de la vie privée », *AJDA*, 2004, p. 2269.

MALAFOSSE J.-B., « Le règlement européen et la protection des données de santé », *Dalloz IP/IT*, 2017, p. 260.

MALAFOSSE J.-B, « A partir de quand peut-on qualifier un logiciel de dispositif médical ? », *Dalloz IP/IT*, 2016, p. 82.

MALAFOSSE J.-B., « Le Conseil d'État demande à l'État d'ouvrir la base de données du SNIIRAM », *Dalloz IP/IT*, 2016, p. 435.

MALLET-POUJOL N., « Protection des données personnelles et droit à l'information », *LEGICOM*, vol. 59, no. 2, 2017, p. 49.

MANFELLOTTO G., « La construction du marché unique numérique entre harmonisation et protection des consommateurs », *Revue de l'Union Européenne*, 2017, p. 418.

MARAIN G., « Le bitcoin à l'épreuve de la monnaie », *AJ contrat 2017*, p. 522.

MARAS M.-H., « Internet of Things : security and privacy implications », *International Data Privacy Law*, Oxford University Press, April 7, 2015.

MARCELLIN S., SEMIK J., « La responsabilité des traitements de données partagés dans un groupe », *Dalloz IP/IT*, 2017, p. 632.

MARCOU G., « La notion juridique de régulation », *AJDA*, 2006, pp. 347-353.

MARINO L., « Le droit d'accès à internet, nouveau droit fondamental », *Rec. Dalloz*, 2009, n° 30, pp. 2045-2046.

MARINO L. et PERRAY R., « Les nouveaux défis du droit des personnes : la marchandisation des données personnelles », in ROCHFELD J. (dir.), *Les nouveaux défis du commerce électronique*, LGDJ – Lextenso éditions, 2010. pp. 55-7.

MARINO L., « To be or not to be connected : ces objets connectés qui nous espionnent », Recueil Dalloz, 2014, p. 29.

MARINO L., « Comment mettre en oeuvre le « droit à l'oubli » numérique ? », *Recueil Dalloz*, 2014, p. 1680.

MARINO L., « Le règlement européen sur la protection des données personnelles : une révolution ! », *La Semaine Juridique*, Edition générale, n°22, 30 mai 2016.

MARTIN A.-C., « Le délit d'obsolescence programmée », *Recueil Dalloz*, 2015, p. 1944.

MARTIAL-BRAZ N., ROCHFELD J., GATTONE E., « Quel avenir pour la protection des données à caractère personnel en Europe ? », *Recueil Dalloz*, 2013, p. 2788.

MARTIAL-BRAZ N., « Objets connectés et responsabilité », *Dalloz IP/IT*, 2016, p. 399.

MARTIAL-BRAZ N., « L'extraterritorialité des décisions des autorités de régulation nationales : gage d'efficacité de la protection des données personnelles en Europe », *Revue de l'Union européenne*, 2016, p. 288.

MARTIAL-BRAZ N., « Les nouveaux droits des individus consacrés par la loi pour une République numérique. Quelles innovations ? Quelle articulation avec le Règlement européen ? », *Dalloz IP/IT*, 2016, p. 525.

MARTIAL-BRAZ N., « Le renforcement des droits de la personne concernée », *Dalloz IP/IT*, 2017, p. 253.

MARTIAL-BRAZ N., « L'abus de textes peut-il nuire à l'efficacité du droit ? », *Dalloz IP/IT*, 2018, p. 459.

MATTATIA F., « CNIL et tribunaux : concurrence ou complémentarité dans la répression des infractions à la loi informatique et libertés ? », *RSC*, 2009, p. 317.

MATTATIA F., YAÏCHE M., « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? », *Lamy Droit de l'Immatériel*, n° 114, 2015, p. 60 à 63.

MAUBENARD C., « La protection des données à caractère personnel en droit européen », *Rev. UE*, 2016, p. 406.

MAXWELL J. W., JACQUIER S. et ZEGGANE T., « Publicité ciblée et protection du consommateur en France, en Europe et aux États-Unis », *CCE*, n° 6, juin 2008, pp. 18-23.

MAXWELL W., LOVELLS H., BOURREAU M., « Les trois facettes de la neutralité technologique », *Les Cahiers de l'ARCEP*, octobre 2014, p. 17.

MAXWELL W., TAÏEB S., « L'accountability, symbole d'une influence américaine sur le règlement européen des données personnelles ? », *Dalloz IP/IT*, 2016, p. 123.

MAZARS M.-F., « La CNIL à l'ère du RGPD : la protection des données personnelles renforcée », *Les Cahiers Sociaux*, n° 306, 1er avril 2018, p. 224.

MAZARS M.-F., EL BOUJEMAOUI W., « Maîtriser le socle du droit de la protection des données pour aborder l'application du Règlement européen (RGPD) », *Rev. trav.*, 2018, p. 298.

MAZEAUD V., « La constitutionnalisation du droit au respect de la vie privée », *Nouveaux Cahiers du Conseil Constitutionnel*, n°48, 2015, p. 7.

MC DONALD M.-A., CRANO F.-L., « The cost of reading privacy policies », *I/S : A Journal of Law and Policy for the Information Society*, vol. 4, no. 3, 2008-2009, pp. 543-568.

METALLINOS N., « Maîtriser le risque Informatique et Libertés », *Droit social*, 2006, p. 378.

METALLINOS 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.

METALLINOS N., « Données personnelles : la CJUE renforce les règles de protection », *Dalloz IP/IT*, 2016, p. 47.

METALLINOS N., « Notification des violations de données à la CNIL : tendre le bâton pour se faire battre ? », *Dalloz IP/IT*, 2016, p. 144.

MEZIANI M., « Le bien-être : enjeux relatifs aux droits et approche pluridisciplinaire », *JS*, 2015, n°151, p. 18.

MOALE-NUYTS C., « Le transfert de données à caractère personnel vers les Etats-Unis conformément au droit européen », *RTD eur.*, 2002, p. 451.

MOLE A., « Au-delà de la loi informatique et libertés », *Droit social*, Dalloz, 1992, p. 603.

MOLE A., « Le nouveau droit des flux transfrontières des données personnelles », *DS*, 2004, n° 12, p. 1072-1076.

MOORE G.-E., « Cramming more components onto integrated circuits », *Electronics*, Volume 38, Number 8, April 19, 1965.

MOREAU Y., DORNBIEBER C., « Enjeux de la technologie de blockchain », *Recueil Dalloz*, 2016, p. 1856.

MORLET-HAÏDARA L., « Le système national des données de santé et le nouveau régime d'accès aux données », *RDSS*, 2018, p. 91.

MOROZOV E., *To Save everything, click here : the folly of technological solutionism*, Hachette UK, mars 2013, p. 36.

MOSSE M., « Quand le Cloud rime avec cybersécurité », *Dalloz IP/IT*, 2016, p. 16.

MOURON P., « De la rumeur aux fausses informations », *Légicom*, 2018, p. 53.

MUCCHIELLI J., « L'e-réputation : préoccupation croissante des Français, pour la CNIL », *Dalloz Actualité*, 20 mai 2014.

MULLIGAN G., « The internet of things : here now and coming soon », *IEEE Internet Computing*, 2010, vol. 14, n° 1, p. 35.

MULTIN A.-L., « Internet - La vente des produits touristiques sur le net, régie par un régime protecteur à l'égard de tous », *Tourisme et Droit*, 2005, n°71, p. 24.

MUNOZ R., « Internet et la protection des données personnelles : un élargissement du champ d'application de la directive 95/46/CE », *Communication Commerce électronique*, n°4, Avril 2004, comm. 46.

NAFTASKI F., DESGENS-PASANAU G., « Enjeux et perspectives du pouvoir de labellisation de la CNIL », *Lamy Droit de l'Immatériel*, 2010, n°63.

NAFUS D., SHERMAN J., « Big Data, Big Questions| This One Does Not Go Up To 11 : The Quantified Self Movement as an Alternative Big Data Practice », *International Journal of Communication*, v. 8, juin 2014, p. 11.

NARAYANAN A., FELTEN W.-E., « No silver bullet : De-identification still doesn't work », *White Paper*, 2014, p. 2.

NELSON P., « Information and Consumer Behavior », *Journal of Political Economy*, vol. 78, n° 2, 1970, pp. 311-329.

NERBONNE S., « Le Groupe de l'article 29 est-il en mesure de s'imposer comme le régulateur des régulateurs par ses prises de position ? », *Legicom*, n° 42, 2009, p. 37 à 46.

NORBERG A. P., HORNE R. D., HORNE A. D., « The privacy paradox : personal information disclosure intentions versus behaviors », *Journal of Consumer Affairs*, Volume 41, Issue 1, march 2007, p. 100 à 126.

OBERDORFF H., « L'espace numérique et la protection des données personnelles au regard des droits fondamentaux », *Revue du Droit public, n°1*, 2016, p. 41.

OCHOA N., « Précisions sur l'article 9 de la loi du 06 janvier 1978 (CE, 11 mai 2015), *Les Petites Affiches*, 7 sept. 2015, n°178, p. 7.

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 », *Revue Française de Droit Administratif*, 2015, p. 1157.

PARICARD S., « La recherche médicale et le droit : une relation ambivalente », *RDSS*, 2009, p. 98.

PASTOR J.-M., « Des données personnelles ne peuvent pas être transmises aux ayants droit », *Dalloz actualité*, 20 juin 2016.

PAULIN B., « La restitution des données : difficultés pratiques », *Dalloz IP/IT*, 2017, p. 33.

PEIGNE J., « La notion de dispositif médical issue du règlement (UE) 2017/745 du 5 avril 2017 », *RDSS*, 2018, p. 5.

PEIGNE J., « Le nouveau cadre juridique des dispositifs médicaux », *RDSS*, 2018, p. 3.

PELLEGRINI F., « La portabilité des données et des services », *RFAP*, 2018, n° 3, p. 513 à 523.

PELLEGRINI F., « Sécurité et hygiène numérique des professionnels », *Dalloz IP/IT*, 2019, p. 233.

PERE D., FOREST D., « L'arsenal répressif du phishing », *Recueil Dalloz*, 2006, p. 2666.

PEREA F., « L'identité numérique : de la cité à l'écran. Quelques aspects de la représentation de soi dans l'espace numérique », *Les Enjeux de l'Information et de la Communication*, Lavoisier, 2010, vol. 1, p. 144 à 159.

PERES C., « Les données à caractère personnel et la mort, Observations relatives au projet de loi pour une République numérique », *Recueil Dalloz*, 2016, p. 90.

PERONNE G., DAOUD E., « Droit à l'oubli contre publicité légale des données : la publicité prime ! », *Dalloz*, IP/IT 2017, p. 345.

PERRAY R., « Quel avenir pour le pouvoir de sanction de la CNIL ? », *Lamy Droit de l'Immatériel*, janv. 2008, n°34, p. 82.

PERRAY R., « La délimitation territoriale du RGDP : le champ d'application et les transferts de données hors de l'Union européenne », *Dalloz IP/IT*, 2016, p. 581.

PERRAY R., « De la (bonne ?) application de la jurisprudence Weltimmo au bénéfice... d'Amazon et de Facebook », *Revue de l'Union européenne*, 2016, p. 597.

PERRAY R., UZAN-NAULIN J., « Existe-t-il encore des données non personnelles ? », *Dalloz IP/IT*, 2017, p. 286.

PEYROU-PISTOULEY S., « L'affaire Marper c/ Royaume-Uni, un arrêt fondateur pour la protection des données dans l'espace de liberté, sécurité, justice de l'Union européenne », *RFDA*, juillet-août 2009, pp. 741-757.

PEYROU S., « Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer : réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne », *Europe*, juillet 2012, pp. 5-9.

PERROU S., « La Cour de justice, garante du droit « constitutionnel » à la protection des données à caractère personnel », *RTD Eur*., janvier-mars 2015, p. 117.

PEYROU-PISTOULEY S., « La protection des données à caractère personnel dans l'ELSJ, work in progress... », *RTD eur*, 2010, p. 775.

PICARD E., « L'émergence des droits fondamentaux en France », *AJDA*, 20 juillet/20 Août 1998, n° spécial, pp. 6-42.

POLIDORI M., « L'arrêt Google Spain de la CJUE du 13 mai 2014 et le droit à l'oubli », *Civitas Europa*, vol. 34, no. 1, 2015, pp. 243-266.

POLLAK M., « La régulation technologique : le difficile mariage entre le droit et la technologie », *RFSP*, Volume 32, n° 2, avril 1982, pp. 165-184.

PONTHOREAU M.-C., « La directive 95/46/CE 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 », *RFDA*, 1997, p. 125.

PONTHOREAU M.-C., « La protection des personnes contre les abus de l'informatique », *Revue Française de droit administratif*, 1996, p. 796.

PONTHOREAU M.-C., « Trois interprétations de la globalisation juridique », *AJDA*, 2006, p. 20.

PONTIER Jean-Marie, « La puissance publique et la prévention des risques », *AJDA*, 6 octobre 2003, pp. 1752-1761.

POSNER A. R., « The right of privacy », *Georgia Law Review*, Vol. 12, Spring 1978, n°3, pp. 393-422.

POULLET Y, « La protection des données : entre libertés, droits subjectifs et intérêts légitimes », in *L'humanisme dans la résolution des conflits*. Utopie ou réalité ?, Liber amicorum Paul Martens, Larcier, 2007, pp.133-150.

POULLET Y., « La loi des données à caractère personnel : un enjeu fondamental pour nos sociétés et nos démocraties ? », *LEGICOM*, 2009/1, N° 42, 2009, p. 47-69.

POULLET Y., 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*, Éditions Karim BENYEKHLEF et Pierre TRUDEL, Thémis, Montréal, 2009, pp. 157-222.

PRADEL J., « L'information personnelle : entre le commerce et les libertés » in *Le droit de la communicatique*, actes du colloque conjoint des facultés de droit de l'Université de Poitiers et de l'Université de Montréal, Éditions Thémis-Université de Montréal- Litec, 1992, pp. 23-42.

PROUST O. ? BARTOLI E., « Les « Binding Corporate Rules » : une solution globale pour les transferts internationaux », *RLDI*, n° 74, août-septembre 2011, pp. 97-102.

QUEMENER M., « Le rôle préventif de la justice en matière de cybersécurité », *Dalloz IP/IT*, 2016, p. 12.

QUESSADA D., « De la sousveillance. La surveillance globale, un nouveau mode de gouvernementalité », *Multitudes*, 2010/1, n° 40, p. 54-59.

QUILLATRE E., THOMAS SERTILLANGES J.-B., « Libre circulation des données à caractère personnel au sein du marché intérieur et de l'espace de liberté sécurité justice : vers une diversification des instruments de régulation », *Petites affiches*, 3 février 2011, n° 24, page 3.

RALLET A., ROCHELANDET F., « Exposition de soi et décloisonnement des espaces privés : les frontières de la vie privée à l'heure du numérique », *Terminal*, n° 105, 2010, p. 71 à 86.

RALLET A., ROCHELANDET F., « La régulation des données personnelles face au web relationnel : une voie sans issue ? », *Réseaux 2011/3*, n° 167, p. 17-47.

RALLET A., ROCHELANDET F., ZOLYNSKI C., « De la Privacy by Design à la Privacy by Using. Regards croisés droit/économie », *Réseaux*, 2015/1, n° 189, p. 15-46.

RAVENEAU G., « Des sports à la jonction de la passion du bien-être et du culte du corps », *JS*, 2015, n°151, p. 25.

RAYNAL F., « De nouvelles dispositions pour protéger les données personnelles », *Documentaliste-Sciences de l'Information*, vol. 51, n°3, 2014.

RENAISSANCE NUMERIQUE, *D'un système de santé curatif à un modèle préventif grâce aux outils du numérique, 16 propositions pour un changement de paradigme des politiques de santé*, Livre Blanc rédigé sous la direction d'Henri Isaac, septembre 2014, 123 p.

REY B., « Les intelligences numériques des informations personnelles. Vers un changement de perspective pour garantir le droit à la vie privée ? », *Les Cahiers du numérique*, 2014/1, Vol. 10, p. 9-18.

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*, juin 2015, n° 48, p. 35.

RICHARD J., CYTERMANN L., « Le droit souple : quelle efficacité, quelle légitimité, quelle normativité ? », *AJDA*, 2013, p. 1884.

RICHARD J., CYTERMANN L., « Le droit souple dans la vie de l'entreprise et de la fonction publique : une tension féconde avec le droit dur », *Droit social*, 2014, p. 400.

RICHARD J., « Le numérique et les données personnelles : quels risques ? quelles potentialités ? », *Revue du droit public*, janvier 2016, n°1, p. 87.

RIDEAU J., « Le rôle de l'Union européenne en matière de protection des droits de l'homme », *RCADI*, Tome 265, pp. 1-480.

RIGAUX François, « La loi applicable à la protection des individus à l'égard du traitement automatisé des données à caractère personnel », *RCDIP*, 1980, pp. 443-478.

RIGAUX François, « L'élaboration d'un « right of privacy » par la jurisprudence américaine », *RIDC*, 1980, n°4, pp.701-730.

ROCHFELD J., « De la « confiance » du consommateur ou du basculement d'un droit de protection de la partie faible à un droit de régulation du marché », *LPA*, 16 février 2009, n° 33, pp. 7-11.

ROCHFELD J., ZOLYNSKI C., « La « loyauté » des « plateformes ». Quelles plateformes ? Quelle loyauté ? », *Dalloz IP/IT*, 2016, p. 520.

ROCHFELD J., « Le « contrat de fourniture de contenus numériques » : la reconnaissance de l'économie spécifique « contenus contre données » », *Dalloz IP/IT*, 2017, p. 15.

ROJINSKY C., « Cyberespace et nouvelles régulations technologiques », *Recueil Dalloz*, 2001, p. 844.

ROMAN D., « A corps défendant », La protection de l'individu contre lui-même, *Rec. Dalloz*, 2007, n° 19, pp. 1284-1293.

ROUVROY A., « Réinventer l'art d'oublier et de se faire oublier dans la société de l'information ? », in *La protection de l'individu numérisé*, Actes du Colloque Asphalès, 22 et 23 novembre 2007, Paris, L' harmattan, 2008, pp. 249-278.

ROUVROY A., BERNS THOMAS, « Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? », *Réseaux*, vol. 177, n°1, 2013, p. 163-196.

ROUYERE A., « La constitutionnalisation des autorités administratives indépendantes : quelle signification ? », *RFDA*, septembre-octobre 2010, pp. 887-895.

ROSEN J., « The right to be forgotten », *Stanford Law Review*, Online, 64, 2011, p. 88.

ROSSI J., « Guide de la jurisprudence européenne en matière de protection des données à caractère personnel », *Cahiers Costech*, mai 2017, n°1, p. 5.

SAADA R., « Plaintes et contrôles sur place : analyse de l'activité de la CNIL et enjeux pour l'avenir », *Dalloz IP/IT*, 2018, p. 217.

SABETE W., « De l'insuffisante argumentation des décisions du Conseil constitutionnel », *AJDA*, 2011, n° 16, p. 885.

SABOURIN P., « Les autorités administratives indépendantes. Une catégorie nouvelle ? », *AJDA*, 1983, pp. 275-295.

SADOU-JARIN L., « La Commission européenne a adopté le bouclier de protection des données transatlantiques », *Dalloz Actualité*, 29 juillet 2016.

SCARAMOZZINO E., « Adoption du bouclier de protection des données UE-EU », *JAC 2016*, n°38, p. 10.

SCARAMOZZINO E., « Les enjeux juridiques du big data », *JT* 2017, n°201, p.35.

SCARAMOZZINO E., « Open data versus protection des données : les enjeux pour le tourisme des smart cities », *Juris Tourisme*, 2018, n°207, p. 24.

SCHWARTZ M. P., « The computer in German and American constitutionnal law : Towards an American right of informational self-determination », *American Journal of Comparative Law*, n° 37, 1989, p. 676.

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.

SENAC C.-E., « Le droit à l'oubli en droit public », *RDP*, n° 4-2012, pp. 1156-1170.

SENECHAL J., « La fourniture de données personnelles par le client via Internet, un objet contractuel ? », *AJ Contrats d'affaires, Concurrence, Distribution*, 2015, p. 212.

SENECHAL J., « Le contrat de fourniture de contenu numérique en droit européen et français : une notion unitaire ou duale ? », *Revue de l'Union européenne*, 2015, p. 442.

SENECHAL J., « La diversité des services fournis par les plates-formes en ligne et la spécificité de leur rémunération, un double défi pour le droit des contrats », *AJCA*, 2016, p. 141.

SENDRA A., « Informatique et Libertés : que change la réforme du 6 août 2004 ? », *in* GIROT J.-L. (dir.), *Le harcèlement numérique*, Dalloz, 2005, pp. 187-207.

SERUGA-CAU E., HAVEL T., « Campagne électorale et utilisation des données personnelles : grands principes et points de vigilance », *AJCT*, 2019, p. 73.

SIMITIS S., « Reviewing privacy in an information society », *University of Pennsylvania Law Review*, vol. 135, n°3, 1987, p. 710.

SIRINELLI P., « Obsolescence reprogrammée », *Dalloz IP/IT*, 2018, p. 1.

SIRINELLI P., PREVOST D., « To be or Notes to be ? », *Dalloz IP/IT*, 2018, p. 205.

SUR Serge, « Vers un nouvel ordre mondial de l'information et de la communication », *AFDI*, 1981, pp. 45-64.

SWAN M., « The quantified-self, Fundamental Disruption in Data Science and Biological Discovery », *MS Futures Group*, Palo Alto, California, Big Data 2013, p. 85.

TEITGEN-COLLY C., « Les instances de régulation et la Constitution », *RDP*, 1990, janvier-février, pp. 153-261.

TESTARD C., « Le droit souple, une « petite source » canalisée, *AJDA*, 2019, p. 934.

THEARD-JALLU C., JOB J.-M., MINTZ S., « Invalidation de l'accord Safe Harbor par la CJUE : portée, impacts et premiers éléments de solution », *Dalloz IP/IT*, 2016, p. 26.

THIBIERGE C., « Le droit souple. Réflexion sur les textures du droit », *RTD Civ.*, Octobre/Décembre 2003, pp. 599-628.

THIERACHE C., « l'agrégation de données ouvertes dans le cadre de plateformes : les objets connectés dans le domaine de la santé », *Legicom*, n° 56, 2016/1, p. 101.

THIERER A., « The Internet of Things and Wearable Technology : Addressing Privacy and Security Concerns without Derailing Innovation », *Richmond Journal of Law & Technology*, 6, 2015.

TIMSIT G., « La régulation. La notion et le phénomène », *RFAP*, 2004, p. 5.

TOMIC Y., « De l'usage des API. Les API de l'Abes », *Documentaliste-Sciences de l'Information*, vol. 51, no. 3, 2014, p. 17.

TRUDEL P., « Quel droit et quelle régulation dans le cyberespace ? », *Sociologie et sociétés*, Volume 32, numéro 2, 2000, p. 191.

TRUDEL P., « Renforcer la protection de la vie privée dans l'État en réseau : l'aire de partage des données personnelles », *RFAP*, n° 110, 2004, pp. 257-266.

TÜRK P., « La souveraineté des États à l'épreuve d'internet », *RDP*, 2013, n° 6, pp. 1489-1521.

USUNIER L., « Du droit commun européen de la vente aux propositions de directives sur les contrats de vente en ligne et de fourniture de contenu numérique : la montagne accouche d'une souris », *RTD Civ*., 2016, p. 304.

VACARIE I., « L'hébergement des données de santé : entre contrat et statut », *RDSS*, 2002, p. 695.

VAYR J., « Les données de santé : un enjeu pour le futur », *Petites affiches*, 16 septembre 2016, n° 185-186, p. 4.

VINEY F., « La loi relative à la protection des données personnelles », *AJ Famille*, 2018, p. 366.

VITALIS A., « L'exercice d'un pouvoir de régulation informatique et libertés et ses difficultés », in PIATTI M.-C. (dir.), *Les libertés individuelles à l'épreuve des NTIC*, PUL, 2001, pp. 143-151.

VIVANT Michel, « Cybermonde : Droit et droits des réseaux », *La Semaine Juridique Edition Générale*, n° 43, 23 Octobre 1996, I 3969, pp. 401-407.

VULLIET-TAVERNIER S., « Après la loi du 6 août 2004 : nouvelle loi « informatique et libertés », nouvelle CNIL ? », *Droit social*, 2004, p. 1055.

WARREN S., BRANDEIS L., « The right to privacy », *Harvard Law Review*, vol. IV, 193, Dec. 15, 1890.

WATSON M.-S., « Living with Data : Personal Data Uses of the Quantified Self », *Oxford Internet Institute*, Masters Thesis, 2013, p. 9.

WEIL P.-A., « Bilan de la CNIL », *Culture Technique*, n°21, Juillet 1990, p. 186.

WEINBAUM N., « Les données personnelles confrontées aux objets connectés », *Communication Commerce électronique*, n°12, décembre 2014.

WINSTON M., PENARD T., « Quelle régulation pour les plateformes numériques en Europe ? », *Annales des Mines - Réalités industrielles*, vol. août 2016, no. 3, 2016, pp. 42-46.

YAYON-DAUVET A., « Le devenir de la protection des données personnelles sur Internet », *Gazette du Palais*, 13 septembre 2001, n° 256, p. 2.

ZOLYNSKI C., « La Privacy by Design appliquée aux Objets Connectés : vers une régulation efficiente du risque informationnel ? », *Dalloz IP/IT*, 2016, p. 404.

ZOLYNSKI C., PUCHERAL P., RALLET A., ROCHELANDET F., « La Privacy by design : une fausse bonne solution aux problèmes de protection des données personnelles ? », *Légipresse*, n° 340, Juillet-Août, 2016, p. 30.

ZOLYNSKI C., « Un nouveau droit de propriété intellectuelle pour valoriser les données : le miroir aux alouettes ? », *Dalloz IP/IT*, 2018, p. 94.

ZOLYNSKI C., LE ROY M., « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », *LEGICOM*, vol. 59, no. 2, 2017, p. 105.

ZORN C., « Contrats de Cloud computing et données personnelles : éléments de rénovation des techniques contractuelles », *Dalloz IP/IT*, 2016, p. 453.

ZOUAG S., « « A grands pouvoirs, grandes responsabilités », *JT*, 2018, n° 204, p. 3 .

B. Contributions à des ouvrages collectifs

AUBY J.-B., « Les *smart cities* : un cadre nouveau pour les politiques sanitaires et les systèmes de santé ? », *in* Antony Taillefait, Maximilien Lanna (dir.), *Smart Cities & Santé*, Institut Universitaire Varenne, « Collection Colloque & Essais », p. 11.

DESGENS-PASANAU G., « Informatique et libertés, une équation à plusieurs inconnues », *in* Jean-Luc Girot (dir.), *Le harcèlement numérique*, Dalloz, 2005, p. 97.

DESWARTE Y., GAMS S., « Protection de la vie privée : principes et technologies », *in Les technologies de l'information au service des droits : opportunités, défis, limites*, Daniel Le Métayer (éd.) Cahiers du centre de recherches Information et Droit, Bruylant, 2010.

FRAYSSINET J., « La protection des données personnelles », *in* A. Lucas, J. Devèze et J. Frayssinet (dir.), *Droit de l'informatique et de l'internet*, PUF, 2001, p. 122.

KAYSER P., « Le Conseil constitutionnel protecteur du secret de la vie privée à l'égard des lois », *in Mélanges offerts à Pierre Raynaud*, Dalloz-Sirey, 1985, p. 329.

LAUDE A., « Le bien-être et le malade », *in* Marta Torre-Schaub (dir.), *Le bien-être et le droit*, Paris, Publications de la Sorbonne, 2016, p. 78.

NAFTALSKY F., « Fichiers des associations et fondations », *in* Philippe-Henri Dutheil (dir.), *Droit des associations et fondations*, Dalloz-Sirey, « Juris corpus », 13 janvier 2016, 1614 p.

IV. OUVRAGES COLLECTIFS, COLLOQUES, CONFERENCES ET MELANGES

ARNAUD J.-A. (dir.), Dictionnaire encyclopédique de théorie et de sociologie du droit, LGDJ, Anthologie du droit, novembre 2018, 758 p.

BELLI L., DE FILIPPI P. (dir.), *Net Neutrality Compendium, Human Rights, Free Competition and the Future of the Internet*, Springer, 2016, 300 p.

BLAIZOT-HAZARD C. (dir.), *NTIC, secret et droits fondamentaux, Les NTIC face aux droits et libertés fondamentaux à travers le prisme du secret,* Institut Universitaire Varenne, Colloques & Essais, 2017, 154 p.

BOURCIER D., DE FILIPPI P. (dir.), *Open Data & Big Data, Nouveaux défis pour la vie privée*, Mare & Martin, Droit & Sciences Politiques, 2016, p. 33.

CASTETS-RENARD C. (dir.), *Quelle protection des données personnelles en Europe*, Larcier, 2015, 190 p.

CONSEIL D'ETAT, *Les agences : une nouvelle gestion publique ?, Un colloque organisé par le Conseil d'Etat le 19 octobre 2012 à l'Ecole nationale d'administration*, La Documentation française, 2013, 140 p.

DELMAS-MARTY M. (dir.), *Critique de l'intégration normative : L'apport du droit comparé à l'harmonisation des droits*, PUF, coll. Les voies du droit, 2004, 320 p.

DUPRE DE BOULOIS X. (dir.), *Les grands arrêts du droit des libertés fondamentales*, Grands arrêts, Dalloz, 2017, 878 p.

GOLDSTEIN B., DYSON L. (dir.), *Beyond Transparency, Open Data and the Future of Civic Innovation*, Code for America Press, 2013, 300 p.

GUTWIRTH S., LEENES R., DE HERT P., POULLET Y. (dir.), *European Data Protection : Coming of Age*, Springer, 2013, 437 p.

HERVE C., STANTON-JEAN M. (dir.), *Innovation en santé publique, des données personnelles aux données massives (big data), Aspects cliniques, juridiques et éthiques*, Dalloz, 2018, 190 p.

HOCHMANN T., JOUVE D., PAILLER P. (dir.), *Le contrôle juridictionnel du droit souple*, Editions et Presses Universitaires de Reims, 2017, 274 p.

MARTIAL-BRAZ N., RIFFARD J.-F., BEHAR-TOUCHAIS M. (dir.), *Les mutations de la norme, Le renouvellement des sources du droit*, coll. « Etudes juridiques », Economica, 2000, 310 p.

MARTIAL-BRAZ N., *L'Extraterritorialité des Décisions des Autorités de Régulation : Gage d'Efficacité de la Protection des Données Personnelles en Europe*, Colloque : La coopération policière, douanière et judiciaire en Europe, Besançon, 24 septembre 2015.

MENGER P.-M., PAYE S. (dir.), *Big Data et traçabilité numérique, Les sciences sociales face à la quantification massive des individus*, Collège de France, coll. « Conférences du Collège de France », 2017, 215 p.

MUNIER M., LALANNE V., ARDOY P.-Y., RICARDE M., « Métadonnées et Aspects Juridiques : Vie Privée vs Sécurité de l'Information », *9ème Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information (SARSSI 2014)*, Mai 2014, Saint-Germain-au-Mont-D'or, France, 2014, p.65-76.

ROUX J., *Détection d'Intrusion dans l'Internet des Objets : Problématiques de sécurité au sein des domiciles*, Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes D'Information (RESSI), Mai 2017, Grenoble, France, 2017, p. 4.

V. DOCUMENTS OFFICIELS, DÉLIBÉRATIONS, RAPPORTS ET AVIS

A. Européens et internationaux

Parlement européen, Commission européenne et Conseil de l'Europe

COMMISSION DES COMMUNAUTÉS EUROPÉENNES, décision n°2001/497/CE du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE [notifiée sous le numéro C (2001) 1539].

COMMISSION DES COMMUNAUTÉS EUROPÉENNES, décision du 27 décembre 2004 modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un

ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers [notifiée sous le numéro C (2004) 5271].

COMMISSION EUROPÉENNE, Communication de la Commission relative à la protection des personnes à l'égard du traitement des données à caractère personnel dans la Communauté et à la sécurité des systèmes d'informations, COM (1990) 314 final du 13 septembre 1990.

COMMISSION EUROPÉENNE, L'application de la décision de la Commission 520/2000/CE du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiées par le ministère du commerce des Etats-Unis d'Amérique, SEC (2002) 196, 13 décembre 2002.

COMMISSION EUROPÉENNE, Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and information security COM (90) 314 final.

COMMISSION EUROPÉENNE, Proposition modifiée de directive 95/46, 15 octobre 1992, COM (90) 422 final.

COMMISSION EUROPÉENNE, Recommandation du 12 mai 2009 sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence [notifiée sous le numéro C (2009) 3200], (2009/387/CE), 16 mai 2009.

COMMISSION EUROPÉENNE, *L'Internet des objets – un plan d'action pour l'Europe*, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, COM (2009), 278 final, Bruxelles, 18 juin 2009, p. 6.

COMMISSION EUROPÉENNE, Décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive

95/46/CE du Parlement européen et du Conseil, C (2010) 593, 2010/87/UE, clause n°8, 12 février 2010.

COMMISSION EUROPÉENNE, Communication de la Commission, Un cadre cohérent pour renforcer la confiance dans le marché unique numérique du commerce électronique et des services en ligne, COM (2011), 942 final/2.

COMMISSION EUROPÉENNE, Communication de la commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Exploiter le potentiel de l'informatique en nuage en Europe, Bruxelles, le 27 septembre 2012, COM (2012) 529 final, p. 3.

COMMISSION EUROPÉENNE, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Les plateformes en ligne et le marché unique numérique, Perspectives et défis pour l'Europe, COM (2016) 172.

COMMISSION EUROPÉENNE, *La Santé en poche : libérer le potentiel de la santé mobile*, Communiqué de Presse, Bruxelles, le 10 avril 2014.

COMMISSION EUROPÉENNE, *Livre vert sur la Santé mobile*, Bruxelles, avril 2014, p. 3.

COMMISSION EUROPÉENNE, *Draft Code of Conduct on privacy for mobile health applications*, June 7th, 2016.

CONSEIL DE L'EUROPE, Rapport explicatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Série des traités européens n° 108, 28 janvier 1981.

CONSEIL DE L'EUROPE, *Les nouvelles technologies : un défi pour la protection de la vie privée ?*, Strasbourg, 1989, p. 35.

CONSEIL DE L'EUROPE, Position commune (CE) nº 1/95 arrêtée par le Conseil le 20 février 1995, JO C 93 du 13.4.1995, p. 20.

CONSEIL DE L'EUROPE, Annexe à la recommandation n° R (97) 5 du Comité des ministres aux Etats-membres relative à la protection des données médicales, adoptée par le Comité des ministres le 13 février 1997, lors de la 584ème réunion des délégués des ministres.

CONSEIL DE L'EUROPE, *Manuel de Droit européen en matière de protection des données*, 2014, p. 105.

DGCCRF, European Commission, *Common position of national authorities within the CPC Network concerning the protection of consumers on social networks*, novembre 2016.

PARLEMENT EUROPÉEN, Résolution du 2 avril 1989 sur la déclaration des droits et libertés fondamentales, JO C 120, 6 mai 1989, p. 51.

PARLEMENT EUROPÉEN, Resolution of the European Parliament on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing [1975] OJ C60/48.

PARLEMENT EUROPÉEN, Resolution of the European Parliament of 8 April 1976 on the protection of the right of the individual in the face of developing technical progress in the field of automatic data processing, OJ [1976] OJ C100/27.

PARLEMENT EUROPÉEN, Resolution of the European Parliament on the protection of the rights of the individual in the face of technical developments in data processing [1979] OJ C140/34.

PARLEMENT EUROPÉEN, Resolution of the European Parliament of 9 March 1982 on the protection of the rights of the individual in the face of technical developments in data processing [1982] OJ C87/39.

PARLEMENT EUROPÉEN, *Rapport sur une durée de vie plus longue des produits : avantages pour les consommateurs et les entreprises*, (2016/2272(INI)), Commission du marché intérieur et de la protection des consommateurs, 9 juin 2017.

POULLET Y., DINANT J.-M., DE TERWANGNE C., *L'autodétermination informationnelle à l'ère de l'Internet*, Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications, Conseil de l'Europe, 2004, 64 p.

G29

G 29, *Document de réflexion, Premières orientations relatives aux transferts de données personnelles vers des pays-tiers – Méthodes possibles d'évaluation du caractère adéquat de la protection*, WP 4, 26 juin 1997, p. 6.

G 29, *5ème rapport annuel pour l'année 2000*, WP54, p. 3.

G 29, *Document de travail relatif aux transferts de données personnelles vers des pays tiers*, 3 juin 2003, WP 74, p. 5.

G 29, *Avis 4/2007 sur le concept de données à caractère personnel*, 01248/07FR WP 136, adopté le 20 juin 2007.

G 29, *Document de travail sur le traitement des données à caractère personnel relatives à la santé, contenues dans les dossiers médicaux électroniques (DME)*, WP 131, 15 février 2007.

G 29, *Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche*, WP 148, adopté le 4 avril 2008.

G29, *Document de travail établissant un cadre pour la structure des règles d'entreprise contraignantes*, WP 154, 24 juin 2008, p. 8.

G 29, *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »*, WP 169, adopté le 16 février 2010, p. 4.

G 29, *Avis 3/2010 sur le principe de la responsabilité*, WP 173, adopté le 13 juillet 2010, p. 6.

G 29, *Avis 8/2010 sur le droit applicable*, WP 179, adopté le 16 décembre 2010, p. 58.

G 29, *avis 9/2011 sur la proposition révisée des entreprises relatives au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID)*, WP 180, 11 février 2011.

G 29, *Avis n° 15/2011 sur la définition du consentement*, WP 187, adopté le 13 juillet 2011.

G 29, *Avis 05/2012 sur l'informatique en nuage*, WP 96, adopté le 1er juillet 2012, p. 2.

G 29, *Avis 03/2013 sur le principe de finalité*, WP 203, adopté le 2 avril 2013.

G 29, *Document explicatif sur les règles d'entreprise contraignantes applicables aux sous-traitants*, WP 204, 19 avril 2013.

G 29, *Avis 03/2014 sur la notification des violations de données à caractère personnel*, 693/14/FR, WP 213, adopté le 25 mars 2014.

G29, *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*, WP 217, adopté le 9 avril 2014.

G 29, *Avis 8/2014 sur les récentes évolutions relatives à l'internet des objets*, 1471/14/FR WP 223, adopté le 16 septembre 2014.

G 29, *Avis 01/2016 sur le projet de décision d'adéquation du Privacy Shield*, WP 238, adopté le 13 avril 2016.

G 29, Lignes directrices relatives au droit à la portabilité des données, WP 242, adoptées le 13 décembre 2016.

G 29, *Lignes directrices sur le délégué à la protection des données*, WP 243, 13 décembre 2016, p. 7.

G 29, *Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant*, Adoptées le 13 décembre 2016, Version révisée et adoptées le 5 avril 2017, 16/FR, WP 244 rev.01, p. 3.

G 29, *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)*, wp247, 4 April 2017.

G 29, *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*, adoptées le 4 avril 2017, WP 248, p. 4.

Autres institutions et organismes

COMMISSAIRE EUROPÉEN Á LA PROTECTION DES DONNÉES, Avis concernant le « Bouclier vie privée UE-États-Unis », Avis 4/2016, 30 mai 2016, p. 3.

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES, Avis du contrôleur européen de la protection des données relatif à la communication de la Commission intitulée « Exploiter le potentiel de l'informatique en nuage en Europe », Bruxelles, 16 novembre 2012, p. 7.

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES, *Résumé de l'avis du Contrôleur européen de la protection des données sur les propositions de la Commission concernant un règlement relatif aux dispositifs médicaux, et modifiant la directive 2001/83/CE, le règlement (CE) no 178/2002 et le règlement (CE) no 1223/2009, et un règlement relatif aux dispositifs médicaux de diagnostic in vitro*, Journal officiel de l'Union européenne, C 358/10, 7 décembre 2013.

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES, « Relever les défis des données massives : Un appel à la transparence, au contrôle par l'utilisateur, à la protection des données dès la conception et à la reddition de comptes », Avis n°7/2015, p. 5.

FTC, *Internet of Things : Privacy & Security in a Connected World*, 9 janvier 2015.

KPMG, *Crossing the line : staying on the right side of consumer privacy*, 2016, p. 7.

OCDE, *Questions d'ordre politique soulevées par la protection des données et des libertés individuelles*, 1976, p. 177.

OCDE, Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, adoptées le 23 septembre 1980.

OECD, *Measuring the Information Economy*, Annex 1., The OECD Definition of the ICT Sector, 2002, p. 81.

OMS, *Cinquante-huitième Assemblée Mondiale de la Santé*, Résolutions et décisions, annexe, Genève, 2005, p. 114.

OMS, *mHealth, New horizons for health through mobile technologies*, Global Observatory for eHealth series, Volume 3, 2011, p. 6.

PRIVACY RIGHTS CLEARINGHOUSE, *Mobile Health and Fitness apps : what are the Privacy Risks*, posted July 2013, Revised December 2014

UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS, *Présentation générale de l'Internet des objets, Secteur de la normalisation des télécommunications de l'UIT*, Y. 2060, juin 2012, p. 1.

B. Français

CNIL

a. Mises en demeure et délibérations

CNIL, décision de la Présidente n° 2015-047 du 21 mai 2015 de mise en demeure publique de la société Google Inc.

CNIL, décision de mise en demeure n°2015-050 du 24 juin 2015.

CNIL, décision de mise en demeure n° 2015-063 du 26 juin 2015.

CNIL, délib. n°80-10 du 01 avril 1980 portant adoption d'une recommandation relative à la mise en œuvre du droit individuel d'accès aux fichiers automatisés.

CNIL, délib. n° 81-94 du 21 juillet 1981 portant adoption d'une recommandation relative aux mesures générales de sécurité des systèmes informatiques.

CNIL, délib. n° 94-095, 15 novembre 1994.

CNIL, délib. n° 96-105 du 3 décembre 1996.

CNIL, délib. n° 98-101, 22 décembre 1998.

CNIL, délib. n° 99-061 du 21 décembre 1999 portant autorisation de mise en œuvre par la revue « Sciences et avenir » d'un traitement de données personnelles de santé à des fins d'analyse statistique des pratiques et des activités de soins.

CNIL, délib. n° 99-062 du 21 décembre 1999 portant autorisation de mise en œuvre par la revue « Le Figaro magazine » d'un traitement de données personnelles de santé à des fins d'analyse statistique des pratiques et des activités de soins.

CNIL, délib. n° 01-011, 08 mars 2001.

CNIL, délib. n° 02-012 du 14 mars 2002.

CNIL, délib. n° 2004-041, 27 mai 2004.

CNIL, délib. n°2005-018, 3 février 2005.

CNIL, délib. n° 2005-045, 15 mars 2005.

CNIL, délib. n°2005-213, 11 octobre 2005.

CNIL, délib. n° 2005-296 du 22 novembre 2005, portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les membres des professions médicales et paramédicales exerçant à titre libéral à des fins de gestion de leur cabinet.

CNIL, délib. n°2006-066 du 16 mars 2006 portant recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules autonomes utilisés par les employés d'un organisme privé ou public.

CNIL, délib. n° 2006-161 du 8 juin 2006, portant adoption de la norme simplifiée n°52.

CNIL, délib. n° 2006-162 du 8 juin 2006, portant adoption de la norme simplifiée n°53.

CNIL, délib. n° 2006-167, 13 juin 2006.

CNIL, délib. n° 2006-203, 14 septembre 2006.

CNIL, délib. n° 2007-006, 18 janvier 2007.

CNIL, délib. n° 2007-106, 15 mai 2007 portant autorisation des applications informatiques nécessaires à la mise en œuvre de la phase expérimentale du dossier pharmaceutique.

CNIL, délib. n° 2007-186, 28 juin 2007.

CNIL, délib. n° 2007-194, 10 juillet 2007.

CNIL, délib. n° 2007-352, 22 novembre 2007.

CNIL, délib. n°2008-005 du 10 janvier 2008 portant autorisation unique de mise en œuvre de traitements automatisés de données relatifs à la gestion des données de santé recueillies dans le cadre de la pharmacovigilance.

CNIL, délib. n° 2008-008 du 22 janvier 2008 autorisant la mise en œuvre par la Ville de Paris et par la Société des Mobiliers Urbains pour la Publicité et l'Information d'un traitement de données à caractère personnel ayant pour finalité la gestion de fichiers de personnes à risques dans le cadre du système de location de vélos Vélib'.

CNIL, délib. n° 2009-474, 23 juillet 2009.

CNIL, délib. n° 2010-112, 22 avril 2010.

CNIL, délib. n°2010-449, 2 décembre 2010 portant autorisation des traitements de données personnelles mis en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du dossier médical personnel.

CNIL, délib. n° 2011-023 du 20 janvier 2011 dispensant des traitements automatisés effectués sur le territoire français par des prestataires agissant pour le compte de responsables de traitement établis hors de l'Union européenne et concernant des données personnelles collectées hors de l'Union européenne.

CNIL, délib. n°2011-205 du 6 octobre 2011 portant avertissement à l'encontre de la société X.

CNIL, délib. n° 2012-176 du 21 juin 2012 portant avertissement à l'encontre de la Société Européenne de Traitement de l'Information (Groupe Crédit Mutuel).

CNIL, délib. n° 2012-431, 6 décembre 2012.

CNIL, délib. n°2013-091, 11 avril 2013 prononçant un avertissement public à l'encontre de la société X.

CNIL, délib. n°2013-227, 18 juillet 2013.

CNIL, délib. n°2013-282, 10 oct. 2013.

CNIL, délib. n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978.

CNIL, délib. n° 2013-420 du 3 janvier 2014 prononçant une sanction pécuniaire à l'encontre de la société X.

CNIL, délib. n° 2014-017 du 23 janvier 2014 portant adoption d'un référentiel pour la délivrance de labels en matière de coffre-fort numérique.

CNIL, délib. n° 2014-239, 12 juin 2014, portant autorisation unique de mise en œuvre, par les professionnels et établissements de santé ainsi que par les professionnels du secteur médico-social habilités par une loi, de traitements de données à caractère personnel ayant pour finalité l'échange par voie électronique de données de santé à travers un système de messagerie sécurisée.

CNIL, délib. n° 2014-293 du 17 juillet 2014 prononçant un avertissement rendu public à l'encontre de la société Régime Coach.

CNIL, délib. n° 2014-298 de la formation restreinte du 7 août 2014 prononçant un avertissement à l'encontre de la société X.

CNIL, délib. n° 2015-165 du 4 juin 2015 portant adoption d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés.

CNIL, délib. n° 2015-414 du 19 novembre 2015 portant avis sur un projet de loi pour une République numérique.

CNIL, délib. n°2016-007 du 26 janvier 2016 mettant en demeure les sociétés X et Y.

CNIL, délib. n° 2016-053, 1 mars 2016.

CNIL, délib. n° 2016-417 du 12 mai 2016 portant avis sur un projet de décret en Conseil d'Etat relatif au dossier médical partagé.

CNIL, délib. n° 2016-108, 21 avril 2016.

CNIL, délib. n° 2016-071, 24 octobre 2016.

CNIL, délib. n° 2016-332 du 10 novembre 2016 autorisant le groupement d'intérêt public Cancéropôle Grand Sud-Ouest à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la mise en œuvre du projet « CLIPP-GSO » d'aide au développement des essais cliniques de phase précoce.

CNIL, délib. n° 2017-001 du 26 janvier 2017.

CNIL, délib. n° 2017-002, 13 avril 2017.

CNIL, délib. n° 2017-006, du 27 avril 2017 prononçant une sanction pécuniaire à l'encontre des sociétés FACEBOOK INC. et FACEBOOK IRELAND.

CNIL, délib. n° 2017-008, 18 mai 2017.

CNIL, décision n° MED-2017-073 du 20 novembre 2017 mettant en demeure la société GENESIS INDUSTRIES LIMITED.

CNIL, délib. n°2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du 6 janvier 1978.

CNIL, délib. n° 2018-326 du 11 octobre 2018 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le règlement général sur la protection des données (RGPD).

b. Autres publications

Guides et fiches pratiques

CNIL, *Les transferts de données à caractère personnel hors Union européenne*, novembre 2012, 38 p.

CNIL, *Comment déterminer la notion d'interconnexion*, Fiche pratique, 5 avril 2011.

CNIL, *Comment permettre à l'homme de garder la main ?, Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, 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, décembre 2017, p. 15.

CNIL, *Comprendre les grands principes de la cryptologie et du chiffrement*, 25 octobre 2016, disponible en ligne à cette adresse : https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement

CNIL, *Critères d'agrément d'organismes de certification pour la certification de délégué à la protection des données (DPO)*, 23 mai 2018.

CNIL, *Les guides de la CNIL : la sécurité des données personnelles*, 2010.

CNIL, *Les guides de la CNIL : guide professionnels de santé*, 2011.

CNIL, *Les guides de la CNIL : la sécurité des données personnelles*, 2017.

CNIL, *Les règles internes d'entreprise ou BCR* (*binding corporate rules*), 2017, p. 2.

CNIL, *Pack de conformité Véhicules connectés et données personnelles*, octobre 2017, p. 16.

CNIL, *PIA, Applications aux objets connectés*, février 2018, 50 p.

CNIL, *Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing*, 25 juin 2012, p. 1.

CNIL et défenseur des droits, *Mesurer pour progresser vers l'égalité des chances*, Guide méthodologique à l'usage des acteurs de l'emploi, 2012, p. 16.

Innovation et prospective

CNIL, « Smartphones et vie privée : pour une nouvelle vision de la protection des données ? », *Lettre Innovation & Prospective de la CNIL*, n°2, février 2012.

CNIL, « Le Quantified self : nouvelle forme de partage des données personnelles, nouveaux enjeux ? », *Lettre Innovation et Prospective*, n° 05, 2013, 4 p.

CNIL, « Les smartphones et leurs apps sous le microscope de la CNIL et d'Inria », *Lettre Innovation & Prospective de la CNIL*, n°8, novembre 2014.

CNIL, « Vie privée à l'horizon 2020. Paroles d'experts », *Cahiers IP Innovation et prospective*, n° 1, 2012, 58 p.

CNIL, « Le corps, nouvel objet connecté, Du quantified-self à la M-Santé : les nouveaux territoires de la mise en données du monde », *Cahiers IP Innovation & Prospective*, n° 2, 2014, 64 p.

Rapports

COMMISSION INFORMATIQUE ET LIBERTÉS, rapport dans le cadre du décret n° 74.938 du 8 novembre 1974 dit « Rapport Tricot », La Documentation française, 1975, tomes 1 et 2.

CNIL, *Bilan et perspectives 1978-1980, Premier Rapport au Président de la République et au Parlement*, La Documentation Française, 1980, p. 9.

CNIL, *Rapport de la Commission Informatique et Libertés*, La Documentation française, 27 juin 1975, p. 17.

CNIL, *7ème rapport d'activité 1986*, La Documentation française, 1986, p. 43.

CNIL, *8ème rapport d'activité 1987*, La Documentation française, 1988, p. 17 et p. 28.

CNIL, *Mesure de la diversité et protection des données personnelles*, Rapport présenté en séance plénière par Madame Anne Debet, 15 mai 2007, p. 14.

CNIL, *Rapport d'activité 2013*, La Documentation française, 2014, p. 17.

Parlement français

BARRET-KRIEGEL B., *L'Etat et la démocratie*, rapport à François Mitterrand, président de la République française, La Documentation française, mars 1986, p. 83.

BLOCHE P., VERCHERE P., *Rapport d'information sur les droits de l'individu dans la révolution numérique*, Assemblée Nationale, n° 3560, 22 juin 2011, p. 14.

DETRAIGNE Y., ESCOFFIER A.-M., *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information*, Rapport d'information fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le

groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques, Sénat, 27 mai 2009, p. 29.

DÉTRAIGNE Y., ESCOFFIER A.-M., Rapport n° 330 du Sénat, session ordinaire de 2009-2010, enregistré à la Présidence du Sénat le 24 février 2010, fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur la proposition de loi de M. Yves DÉTRAIGNE et Mme Anne-Marie ESCOFFIER visant à mieux garantir le droit à la vie privée à l'heure du numérique.

FRISON-ROCHE M.-A, *Étude dressant un bilan des autorités administratives indépendantes*, in GELARD P., *Les autorités administratives indépendantes : évaluation d'un objet juridique non identifié*, Rapport établi au nom de l'office parlementaire d'évaluation de la législation, Assemblée nationale n° 3166, Sénat n° 404, [2005-2006], juin 2006, Tome 2.

GELARD P., *Les autorités administratives indépendantes : évaluation d'un objet juridique non identifié*, Rapport établi au nom de l'office parlementaire d'évaluation de la législation, Assemblée nationale n° 3166, Sénat n° 404, [2005-2006], juin 2006, Tome 1 et 2, 138 p.

GORCE G., PILLET F., Rapport n° 469 du Sénat, session ordinaire de 2013-2014, Enregistré à la Présidence du Sénat le 16 avril 2014, fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur l'open data et la protection de la vie privée, 85 p.

JOISSAINS S., *Rapport fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi, adopté par l'Assemblée Nationale après engagement de la procédure accélérée, relatif à la protection des données personnelles*, Sénat, n° 350, 14 mars 2018, p. 198.

LASSERRE B., *L'État et les technologies de l'information et de la communication : vers une administration à accès pluriel*, Commissariat général du Plan, La Documentation française, 2000, 194 p.

LE DAIN A.-Y, SIDO B., *Sécurité numérique et risques : enjeux et chances pour les entreprises*, Les Rapports de l'OPECST, La Documentation Française, Février 2015, 370 p.

LE DAIN A.-Y., GOSSELIN P., *Rapport d'information sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française*, n° 4544, 22 février 2017, p. 30.

PAUL C., FERAL-SCHUHL C., Commission de réflexion et de propositions ad hoc sur le droit et les libertés à l'âge du numérique, *Rapport Numérique et libertés : un nouvel âge démocratique*, n° 3119 déposé le 9 octobre 2015 par M. Christian Paul et Mme Christiane Féral-Schuhl, co-Présidents de la Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique, au nom de cette commission.

THYRAUD J., *Rapport fait au nom de la Commission des Lois constitutionnelles, de Législation, du Suffrage universel, du Règlement et d'Administration générale, sur le projet de loi, adopté par l'Assemblée Nationale, relatif à l'informatique et aux libertés*, Sénat, Première session ordinaire de 1977-1978, n° 72, p. 8.

TÜRK A., *Rapport fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi, adopté par l'Assemblée nationale, relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, Sénat, n° 218, 19 mars 2003, 324 p.

Conseil d'Etat

CONSEIL D'ÉTAT, *Sur le principe de transparence*, La Documentation française, collection études et documents n° 47, 1995, 617 p.

CONSEIL D'ÉTAT, *Internet et les réseaux numériques*, La Documentation française, 1998, 193 p.

CONSEIL D'ÉTAT, *Considérations générales sur les AAI : EDCE*, n° 52, Rapport public 2001, La Documentation française, 2001, 471 p.

CONSEIL D'ÉTAT, *Inventaire méthodique et codification du droit de la communication*, La Documentation française, 2006, 446 p.

CONSEIL D'ÉTAT, *Les agences : une nouvelle gestion publique*, Etude Annuelle 2012, La Documentation Française, 2012, p. 12.

CONSEIL D'ÉTAT, *Le droit souple*, Etude annuelle 2013, La Documentation Française, 2012, p. 61.

CONSEIL D'ÉTAT, *Le Numérique et les droits fondamentaux*, *Etude annuelle 2014*, La Documentation Française, 2014, 441 p.

CONSEIL D'ÉTAT, *Puissance publique et plateformes numériques : accompagner l'« ubérisation »*, *Etude annuelle 2017*, La documentation française, 2017, p. 26.

GAZIER F., CANNAC Y., *Etude sur les autorités administratives indépendantes*, éd. La documentation Française, coll. « Etudes et documents du Conseil d'Etat », n°35, 1983-1984, p. 22.

Autres institutions et organismes

AFCDP, *Document de base sur la conservation des données*, 2011, p. 1.

AFCDP, *Quantified Self connecté et Informatique & Libertés*, Synthèse des travaux du sous-groupe « Quantified Self », du groupe de travail « Données de santé » de l'AFCDP, Novembre 2015, p. 14.

AFCDP, « La blockchain est-elle soluble dans le RGPD ? », Compte-rendu de l'intervention de Bruno Rasle, délégué général de l'AFCDP, lors de l'assemblée générale de l'AFCDP qui s'est tenue à Paris le 21 juin 2017, disponible en ligne à cette adresse : https://www.afcdp.net/La-Blockchain-est-elle-soluble

AFNOR, *Management des risques – approche globale*, guide ISO/IEC 73, Recueil Norme et réglementation, Editions Afnor, décembre 2009, 560 p.

AFNOR, *Guide Protection des Données personnelles : l'apport des normes volontaires*, janvier 2017, p. 19.

ANSM, *Logiciels et applications mobiles en santé*, Point d'information, 5 mai 2015, disponible en ligne à cette adresse : http://ansm.sante.fr/S-informer/Points-d-information-Points-d-information/Logiciels-et-applications-mobiles-en-sante-information-des-utilisateurs-Point-d-information

ANSSI, *Maîtriser les risques de l'infogérance : externalisation des systèmes d'information,* décembre 2010, p. 8.

ANSSI, Recommandations pour la sécurisation des sites web, 13 août 2013.

ANSSI, Recommandations de sécurité relatives aux ordiphones, 28 juillet 2015.

ARCEP, *Etude sur le périmètre de la notion d'opérateur de communications électroniques*, Etude réalisée par les cabinets Hogan Lovells et Analysys Mason pour le compte de l'ARCEP, Les actes de l'ARCEP, juin 2011, p. 49.

ARCEP, *Internet des objets : inventer une régulation pro innovation*, Conférence de l'Arcep, 7 novembre 2016.

ARCEP, *Préparer la révolution de l'Internet des objets*, Livre Blanc, 7 novembre 2016, p. 2.

AUTORITE DE LA CONCURRENCE, *Note sur le projet de loi pour une République numérique*, 10 novembre 2015, p. 8.

BOIZARD M., BLANDIN A., CORGAS C, DEDESSUS Le MOUSTIER G., GAMBS S., LEJEALLE C, MOISDON-CHATAIGNER S., PIERRE P., PIOLLE G., ROUSVOAL L., *Le droit à l'oubli*, rapport élaboré pour le GIF de la Mission de recherche Droit et Justice, février 2015, p. 13.

BEGAUD B., POLTON D., VON LENNEP F., L*es données de vie réelle, un enjeu majeur pour la qualité des soins et la régulation du système de santé, L'exemple du médicament*, Rapport réalisé à la demande de Madame la Ministre de la santé Marisol Touraine, Rapport final, mai 2017, p. 47.

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, 3 mars 1998, p. 1.

BRAIBANT Guy, *Données personnelles et société de l'information*, Rapport au Premier ministre, La Documentation française, Collection des rapports officiels, 1998, 292 p.

BURNEL P., VON LENNEP F., *Commission Open Data en santé*, rapport remis à Marisol Touraine, Ministre des Affaires sociales et de la santé, La Documentation Française, 9 juillet 2014.

CURIEN N., MUET P.-A., *La société de l'information*, Rapport de La Documentation française. Paris, 2004, 310 p.

CENTRE D'ANALYSE STRATEGIQUE, *Le dispositif médical innovant*, La Documentation française, 2013, p. 51.

CESE, *Les données numériques : un enjeu d'éducation et de citoyenneté*, avis présenté par M. Éric Peres, rapporteur au nom de la section de l'éducation, de la culture et de la communication, 2015, p. 12.

CESE, *Réseaux sociaux numériques : comment renforcer l'engagement citoyen ?*, avis présenté par M. Gérard Aschieri et Mme. Agnès Popelin, janvier 2017, p. 30.

CONSEIL NATIONAL DU NUMERIQUE, *Rapport sur la neutralité des plateformes*, mai 2014, p. 37.

CONSEIL NATIONAL DU NUMERIQUE, *La Santé, bien commun de la société numérique. Construire le réseau du soin et du prendre soin*, Rapport remis à la

Ministre des Affaires sociales, de la Santé et des Droits des femmes, Octobre 2015, p. 7.

CONSEIL NATIONAL DU NUMERIQUE, Avis n° 2015-3 relatif au projet de loi pour une République numérique, 30 novembre 2015, p. 2 et p. 7.

CONSEIL NATIONAL DU NUMERIQUE, *Avis sur la libre circulation des données dans l'Union européenne*, avril 2017, p. 3.

CONSEIL NATIONAL DU NUMERIQUE, Pourquoi le Privacy Shield doit être renégocié, Communiqué, mardi 19 septembre 2017, disponible en ligne à cette adresse : https://cnnumerique.fr/pourquoi-le-privacy-shield-doit-etre-renegocie

CONSEIL NATIONAL DE L'ORDRE DES MEDECINS, *Santé Connectée, De la E-Santé à la Santé Connectée, Le Livre Blanc du Conseil National de l'Ordre des médecins*, janvier 2015, p. 9.

COUR DES COMPTES, *Les données personnelles de santé gérées par l'assurance maladie, Une utilisation à développer, une sécurité à renforcer*, Communication à la commission des affaires sociales et à la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale de l'Assemblée nationale, mars 2016, p. 97.

DIGITAL SECURITY ECONOCOM, *La sécurité de l'Internet des objets*, Livre Blanc, 2017, p. 23.

GÉNÉRATION LIBRE, *Mes data sont à moi. Pour une patrimonialité des données personnelles*, janvier 2018, p. 8.

HAUTE AUTORITE DE SANTÉ, *Parcours du dispositif médical en France*, Guide pratique, novembre 2017, p. 12.

INSTITUT MONTAIGNE, *Big Data et objets connectés, Faire de la France un champion de la Révolution Numérique*, avril 2015, p. 69.

NOUVELLE FRANCE INDUSTRIELLE, *Internet des Objets*, 14 décembre 2016, p. 6.

RENAISSANCE NUMÉRIQUE, *D'un système de santé curatif à un modèle préventif grâce aux outils numériques*, 16 propositions pour un changement de paradigme des politiques de santé, septembre 2014, p. 35.

PON D., COURY A., *Stratégie de transformation du système de santé – Rapport final : Accélérer le virage numérique*, Ministère des solidarités et de la santé, septembre 2018, 33 p.

TRUCHE P., FAUGERE J.-P., FLICHY P., *Administration électronique et protection des données personnelles*, Ministère de la fonction publique, La Documentation Française, février 2002, 129 p.

VI. JURISPRUDENCE

A. Juridictions supranationales

1. CEDH et Comm. EDH

CEDH, *Z. c. Finlande*, requête 22009/93, 27 juillet 1997.

CEDH, *L.L. c. France*, requête n° 7508/02, 12 février 2007.

CEDH, *S. et Marper c. Royaume-Uni*, requêtes n° 30562/04 et 30566/04, 4 décembre 2008.

CEDH, *Amann c. Suisse*, requête n° 27798/95, 16 février 2000.

CEDH, *Rotaru c. Roumanie*, requête n° 28341/95, 4 mai 2000.

CEDH, *Khelili c. Suisse*, requête n° 16188/07, 18 octobre 2011.

CEDH, *Delfi AS c. Estonie*, requête n° 64569/09, 15 juin 2005.

CEDH, *Magyar Helsinki Bizottsàg c. Hongrie*, requête n° 18030/11, 8 novembre 2016.

2. Juridictions de l'Union européenne

CJCE, 26 avril 1994, *Roquette Frères*, aff. C-228/92.

CJUE, 6 novembre 2003, *Bodil Lindqvist*, C-101/01.

CJUE, 9 novembre 2010, G. Ch., *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen*, Affaires jointes C-92/09 et C-93/09.

CJUE, 24 novembre 2011, G. Ch., *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10.

CJUE, 22 novembre 2012, *Brain Products GmbH c. BioSemi VOF*, aff. C-219/11.

CJUE, 30 mai 2013, *Worten* c. ACT, C-342/12.

CJUE, 11 décembre 2013, *Frantisek Rynes*, C-212/13.

CJUE, 8 avril 2014, *Commission c. Hongrie*, C-288/12.

CJUE, 13 mai 2014, G. Ch., *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, C-131/12.

CJUE, 1er oct. 2015, *Weltimmo s.r.o. c/ Nemzeti Adatvédelmi és Információszabadság Hatóság*, aff. C-230/14.

CJUE, 6 oct. 2015, G. Ch., *Schrems c. Data Protection Commissioner*, C-362/14.

CJUE, 19 oct. 2016, 2ème Ch., *Patrick Breyer c. Bundesrepublik Deutschland*, C-582/14.

CJUE, 21 décembre 2016, *Tele2 Sverige*, C-203/15 et C-698/15.

CJUE, 25 jan. 2018, *Maximilian Schrems c/ Facebook Ireland Limited*, C-498/16.

B. Juridictions françaises

1. Conseil Constitutionnel

CONSEIL CONSTITUTIONNEL, 28 juillet 1989, n° 89-260 DC, *Loi relative à la sécurité et à la transparence du marché financier*.

CONSEIL CONSTITUTIONNEL, 30 décembre 1997, n° 97-395 DC, *Loi de finances pour 1998*.

CONSEIL CONSTITUTIONNEL, 14 décembre 2006, n° 2006-544 DC, *Loi de financement de la sécurité sociale pour 2007*.

CONSEIL CONSTITUTIONNEL, 10 juin 2009, n° 2009-580 DC, *Loi relative à la diffusion et à la protection de la création sur Internet*.

CONSEIL CONSTITUTIONNEL, 23 juillet 1999, n° 99-416 DC, *Loi portant création d'une couverture maladie universelle*.

CONSEIL CONSTITUTIONNEL, 21 décembre 1999, n° 99-422 DC, *Loi de financement de la sécurité sociale pour 2000*.

CONSEIL CONSTITUTIONNEL, 22 mars 2012, n° 2012-652 DC, *Loi relative à la protection de l'identité*, considérant 8.

CONSEIL CONSTITUTIONNEL, 16 juin 2017, n°2017-637 QPC, *Assoc. Nationale des supporters*.

2. Conseil d'Etat et juridictions administratives

CE, 5 juin 1987, n° 59674, *Kaberseli*, publié au recueil Lebon.

CE, 14 octobre 1991, n° 90260, *Section régionale « Normandie Mer du Nord » du comité interprofessionnel de conchyliculture et Quetier*, publié au recueil Lebon.

CE, 17 février 1992, n° 73230, *Société Textron*, publié au recueil Lebon.

CE, 26 juillet 1996, n° 160481, mentionné aux tables du recueil Lebon.

CE, 6 janvier 1997, n° 159129, *Caisse d'épargne Rhône-Alpes Lyon c. CNIL*, publié au recueil Lebon.

CE, 30 juillet 1997, n°182400.

CE, 3 décembre 1999, n° 197060 et n° 197061.

CAA Douai, 1re ch., 17 mai 2001, n° 99DA020329.

CE, 30 octobre 2001, n° 204909, publié au recueil Lebon.

CE, 28 juillet 2004, n° 262851, *Fathy X…c/ CNIL*, publié au recueil Lebon.

CE, 19 février 2008, référé, *Société Profil France*, n° 311974.

CE, 19 juillet 2010, n° 317182, *Fristot et Mme Charpy*, publié au recueil Lebon.

CE, 26 novembre 2010, n° 323694, *Monsieur A. et a*, publié au recueil Lebon.

CE, 21 mars 2011, n° 329879, *Syndicat national du contrôle technique automobile*, publié au recueil Lebon.

CE, 12 mars 2014, n° 354629, *Société Foncia Groupe.*

CE, 11 avr. 2014, n°348111, *Juricom et associés c. CNIL*, inédit au recueil Lebon.

CE, 26 mai 2014, n°354903, *Sté IMS Health*, Mentionnée au Recueil Lebon.

CE, 23 mars 2015, n° 357556, mentionné dans les tables du recueil Lebon.

CE, 9 novembre 2015, n° 384673, publié au recueil Lebon 2015.

CE, 21 mars 2016, n° 368082, *Fairvesta International*, publié au recueil Lebon.

CE, 21 mars 2016, n° 390023, *Numéricable*, publié au recueil Lebon.

CE, 8 février 2017, n° 393714, Mentionné dans les tables du recueil Lebon.

CE, 15 décembre 2017, n° 403776, publié au recueil Lebon 2017.

3. Cour de cassation et juridictions judiciaires

Cour de cassation

Cass. Ass. 7 mars 1986, pourvoi n° 83-10477, publié au bulletin.

Cass. Soc., 10 juillet 2002, pourvoi n° 00-40209, publié au bulletin.

Cass. Crim., 28 septembre 2004, pourvoi n° 03-86.604, Bull. crim. N° 224.

Cass. Crim., 22 octobre 2014, pourvoi n° 13-82.630.

Cass. Crim., 14 mars 2006, pourvoi n° 05-83.423, *Bull. crim*. N° 69.

Cass. 1re civ., 3 novembre 2016, pourvoi n° 15-22.595 (à paraître).

Cours d'appel

CA Paris, 17 septembre 2004, *Ministère public et autres / Jean-Louis C.*

CA Aix-en-Provence, 21 septembre 2005, n° 05/21115.

CA Paris, 15 mai 2007, *S. c/ Min. public et a.*

CA Pau, 23 mars 2012, *Sébastien R. / Facebook.*

CA Paris, 24 février 2015, *J.-C. D. et La Closerie des Lilas / Ministère public et J.-M. T.*

CA Paris, 12 février 2016, *Facebook Inc./ Monsieur X.*

Juridictions de première instance

TGI Seine, 4 octobre 1965, JCP 1966 II, 14482, obs. Lyon-Caen.

TGI Bayonne, 15 novembre 2005, *Ministère public, Scpp / Didier T.*

TGI Bobigny, 14 décembre 2006, *Laurent F. / Sacem.*

TGI Saint-Brieuc, 6 septembre 2007, *Ministère public, SCPP, SACEM / J.-P.*

TGI Paris, ord. réf., 25 juin 2009, n° 09/55437.

TGI Montpellier, 28 octobre 2010, *Marie C. / Google Inc. et Google France.*

T. COM. Paris, 1re ch., 28 janv. 2014, *M. X. / Google Inc. et Google France.*

TGI Paris, ord. réf., 16 septembre 2014, *M. et Mme X et M. Y / Google France.*

TGI Paris, ord. réf., 19 décembre 2014, *Marie-France M. / Google France et Google Inc.*

TGI Paris, ord. réf., 23 mars 2015, *M. P. / 20 Minutes France***.**

VII. Liens en ligne

Elsa Trujillo, « La Chine commence déjà à mettre en place son système de notion des citoyens prévu pour 2020 », Le Figaro, 27 décembre 2017, accessible en ligne à cette adresse : http://www.lefigaro.fr/secteur/high-tech/2017/12/27/32001-20171227ARTFIG00197-la-chine-met-en-place-un-systeme-de-notation-de-ses-citoyens-pour-2020.php

Geoffray Sylvain, « AXA conditionne un avantage santé à un objet connecté », Aruco, 3 juin 2014, disponible en ligne à cette adresse : https://aruco.com/2014/06/axa-objet-connecte/

Jean-Philippe Foegle, « La CJUE, magicienne européenne du « droit à l'oubli » numérique », La Revue des droits de l'homme [En ligne], Actualités Droits-Libertés, mis en ligne le 16 juin 2014, consulté le 03 août 2018.

VIII. Presse

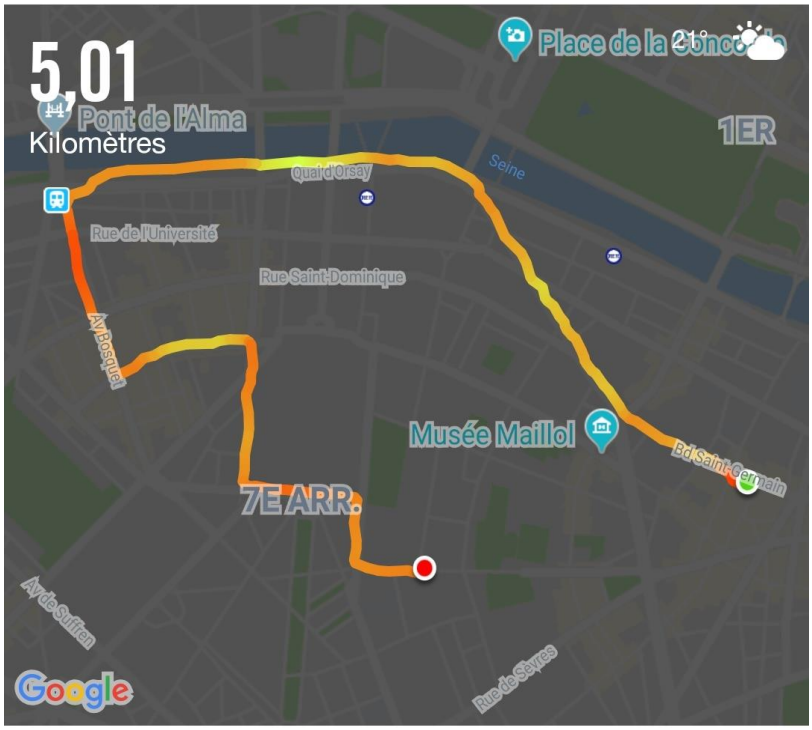
Philippe Boucher, « SAFARI ou la chasse aux Français », Le Monde, 21 mars 1974.

Le Monde, « L'assemblée inscrit la « protection » des données personnelles dans la Constitution, 19 juillet 2018, accessible en ligne à cette adresse : https://www.lemonde.fr/pixels/article/2018/07/19/l-assemblee-inscrit-la-protection-des-donnees-personnelles-dans-la-constitution_5333463_4408996.html

Table des annexes

Annexe 1

Capture d'écran de l'application Nike+ Run Club



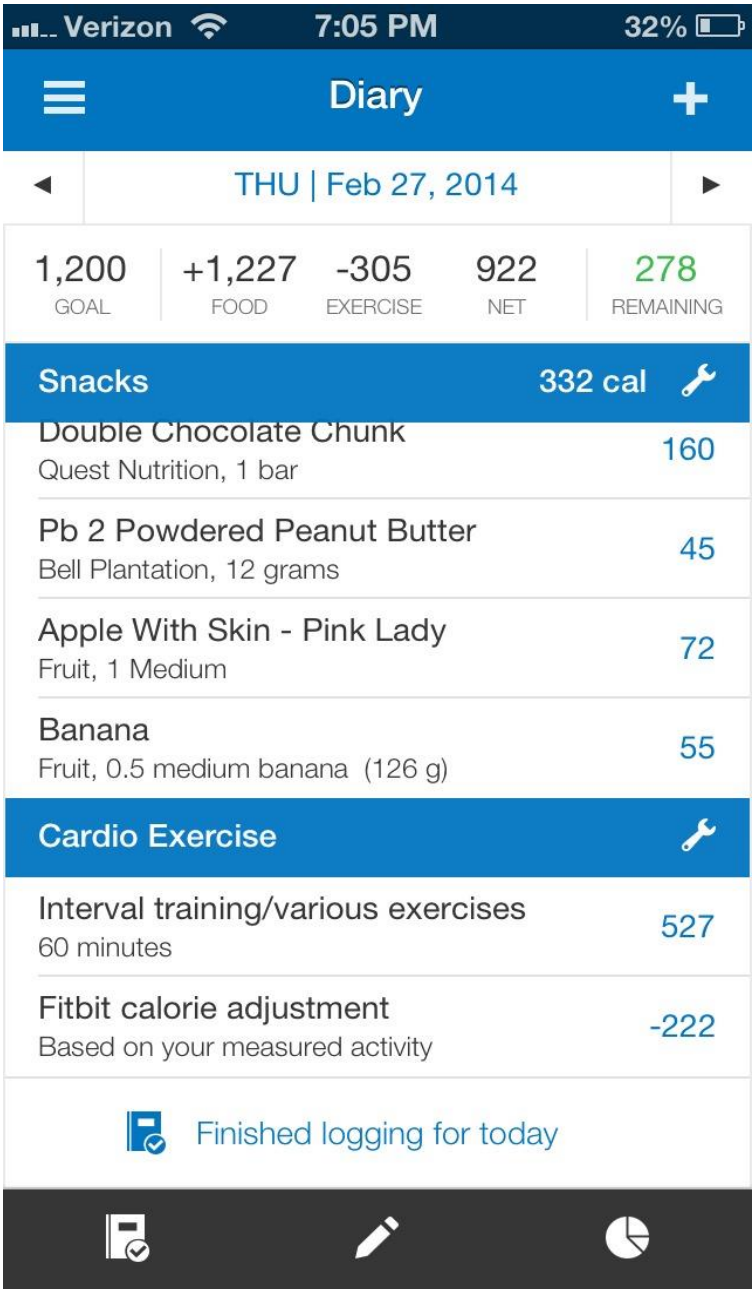
DÉTAILS ET TEMPS INTERMÉDIAIRES

5,01 Kilomètres	**4'56"** Allure moy.	**24:42** Durée
-- Dénivelé	**--** Rythme cardiaque	**382** Calories estimées

Annexe 2

Capture d'écran de l'application My Fitness Pal

(Source : foodielovesfitness.com)



Index

D

E

F

G

L

M

O

P

R

S

TABLE DES MATIÈRES

RÉSUMÉ

Le droit des données à caractère personnel est aujourd'hui un droit en pleine mutation. La protection qu'il est censé conférer aux individus est confrontée à l'apparition de nouvelles pratiques reposant sur l'utilisation de dispositifs permettant une collecte à grande échelle de données à caractère personnel. S'inscrivant dans ce cadre, la pratique de l'automesure connectée ou *quantified-self* a contribué, par ses modalités de fonctionnement, à une remise en cause des principes protecteurs instaurés depuis la fin des années 1970 par la loi Informatique et Libertés.

Cette étude poursuit un double objectif. Tout d'abord, faciliter l'identification des situations dans lesquelles la pratique de l'automesure connectée met à mal certains principes fondamentaux de la protection des données, de façon à pouvoir mettre en lumière les risques auxquels les individus sont soumis. Ensuite, identifier les mutations du cadre juridique lorsque celui-ci est confronté au développement des technologies employées pour la pratique de l'automesure : ces technologies conduisent à une technicité croissante du droit et favorisent, conformément aux mécanismes instaurés par le RGPD, le développement d'une régulation co-construite par les différents acteurs du secteur.

Descripteurs : Informatique et Libertés ; Objets connectés ; Automesure connectée ; Quantified Self ; Régulation.

Personal data protection law and quantified-self :

Personal data protection law is today at a turning point : its core principles are weakened by self-tracking technologies, thus reducing protection of individuals. In order to determine how new technologies affect the law, this study aims to figure ou the paradigm shift that has been implemented by the new RGPD and its consequences on personal data protection.

Keywords : Personal Data Protection ; Quantified-self ; Self-tracking ; RGPD ; Soft-Law.