Parlement européen

Le droit au respect de la vie privée : les défis digitaux,

une perspective de droit comparé

France

ÉTUDE

EPRS | Service de recherche du Parlement européen

Unité Bibliothèque de droit comparé
PE 628.241 – octobre 2018

FR

LE DROIT AU RESPECT DE LA VIE PRIVÉE : LES DÉFIS DIGITAUX, UNE PERSPECTIVE DE DROIT COMPARÉ

France

ÉTUDE

octobre 2018

Résumé

La présente étude fait partie d'un projet plus général qui vise à jeter les bases d'une comparaison des régimes juridiques applicables au droit au respect de la vie privée dans les différents ordres juridiques, ainsi que des solutions prévues par ces ordres juridiques pour répondre aux enjeux que l'« ère digitale » pose à ce droit.

Les pages ci-après exposent, relativement à la France et en rapport avec le thème de l'étude, la législation en vigueur, la jurisprudence la plus pertinente et la nature du droit au respect de la vie privée, et s'achèvent par quelques conclusions sur les enjeux précités.

Reconnu tardivement en droit français, le droit au respect de la vie privée a été consacré par le législateur en 1970. Au contenu insaisissable, ce droit a été adapté aux évolutions technologiques de manière à poser des limites aux intrusions dans la sphère privée : tout d'abord face aux avancées de l'informatique avec la grande loi de 1978, puis à celles du numérique en adaptant cette même loi. Bien que la Constitution de 1958 reste silencieuse, le Conseil constitutionnel a consacré comme fondamental le droit au respect de la vie privée et pose des limites aux intrusions dans la sphère privée.

AUTEUR

Ce document a été rédigé par **Prof. Dr. Marie-Claire Ponthoreau,** Professeur de droit public à l'Université de Bordeaux, à la demande de l'Unité Bibliothèque de droit comparé, Direction générale des services de recherche parlementaire (DG EPRS), Secrétariat général du Parlement européen.

ADMINISTRATEUR RESPONSABLE

Prof. Dr. Ignacio Díez Parra, chef de l'Unité Bibliothèque de droit comparé
Pour contacter l'Unité, veuillez écrire à l'adresse : EPRS-ComparativeLaw@europarl.europa.eu

VERSIONS LINGUISTIQUES

Original : FR

Traductions : DE, EN, ES, IT

Ce document est disponible sur Internet à l'adresse suivante : http://www.europarl.europa.eu/thinktank

Manuscrit achevé en août 2018

Bruxelles © Union européenne, 2018.

PE 628.241

Papier	ISBN 978-92-846-3917-5	DOI:10.2861/231598	QA-04-18-839-FR-C
PDF	ISBN 978-92-846-3915-1	DOI:10.2861/779730	QA-04-18-839-FR-N

Table des Matières

Liste des abréviations

aff.	affaire
AJDA	Actualité Juridique. Droit Administratif
ass.	assemblée
CE	Conseil d'État
CEDH – Cour EDH	Cour européenne des droits de l'homme
Civ. 1ère	Chambre civile
CJUE	Cour de justice de l'Union européenne
CNCDH	Commission nationale consultative des droits de l'homme
CNCTR	Commission nationale de contrôle des techniques de renseignements
CNIL	Commission nationale de l'informatique et des libertés
Coll.	Collection
D.	Dalloz
DC	Décision de contrôle de constitutionnalité des lois
éd.	Édition
et a.	et autres
FAED	Fichier automatisé des empreintes digitales
FBI	« Federal Bureau of Investigation » (Bureau fédéral d'enquêtes des États-Unis)
GAFAM	Google, Apple, Facebook, Amazon, Microsoft
JCP G	La semaine juridique édition générale
JORF	Journal Officiel de la République Française
NCCC	Nouveaux cahiers du Conseil constitutionnel
n°	numéro
NSA	« National Security Agency » (Agence de sécurité nationale des États-Unis)
p.	page
pp.	pages
PRISM	Programme de surveillance électronique (des États-Unis)
PUF	Presses universitaires de France
QPC	Question prioritaire de constitutionnalité
Rapport AN	Rapport de l'Assemblée nationale
RGPD	Règlement général sur la protection des données
RDP	Revue du droit public et de science politique

RFDA	Revue française de droit administratif
STIC	Système de traitement des infractions constatées
TAJ	Traitement d'antécédents judiciaires
vol.	volume

Synthèse

Apparu entre le XVIIIe et le XIVe siècles, le droit au respect de la vie privée est sans contenu légal. Reconnu tardivement en droit français, il est consacré par le législateur en 1970. La vie privée continue d'avoir un contenu insaisissable qui entrave toute tentative de la définir de manière exhaustive. Ce droit s'est adapté aux évolutions technologiques : tout d'abord aux avancées de l'informatique, puis à celles du numérique. La France a adopté en 1978 une loi pour protéger les individus contre les abus de l'informatique. La prospérité du dispositif mis en place tient à sa capacité à s'adapter et à protéger les individus contre les intrusions dans leur sphère privée. Précisément, la sphère d'autonomie dont disposent les individus est bouleversée à l'ère digitale. D'un côté, le numérique est un nouvel *espace de libertés*. En particulier, les libertés d'information et d'expression acquièrent une portée ignorée jusqu'alors puisque d'un seul 'clic', la communication peut être établie avec un nombre considérable de personnes. De l'autre, la numérisation est aussi constitutive d'un *espace contre les libertés* en donnant des possibilités de collecte, de stockage et d'exploitation des données personnelles sans commune mesure avec celles qui existaient auparavant (le *Big data* permettant une collecte massive des données sans finalité précise). Correctement mis en question, même les données les plus inoffensives, une fois recueillies, peuvent révéler des informations sensibles. De telles ressources ont fini par attirer les gouvernements, qui sont de plus en plus à la recherche d'informations pour anticiper les menaces potentielles, en particulier, en matière de la sécurité publique. À l'instar de nombreuses assemblées parlementaires, le parlement français a amplifié l'arsenal législatif de manière à lutter contre le terrorisme. Le Conseil constitutionnel exerce son contrôle de constitutionnalité des lois (*a priori* ou bien *a posteriori* avec la question prioritaire de constitutionnalité) sur un droit qui n'est pas expressément reconnu par la Constitution de 1958 : ni le droit au respect de la vie privée, ni le droit à la protection des données personnelles ne bénéficient d'une base textuelle. Ces droits ont été consacrés de manière progressive par le Conseil constitutionnel qui a tâtonné avant de reconnaître le droit au respect de la vie privée comme droit fondamental, puis de lui rattacher le droit à la protection des données personnelles. Ce dernier droit est un prolongement du premier et ne semble pas être autonome par rapport à celui-ci. Puisque le respect de la vie privée n'est pas absolu, il doit être concilié avec d'autres droits ou principes constitutionnels légitimes. Le Conseil constitutionnel exerce un contrôle de proportionnalité. Le débat autour d'une reconnaissance constitutionnelle explicite et séparée des droits au respect de la vie privée et de la protection des données personnelles est récurrent car cette reconnaissance pourrait à la fois clarifier le fondement constitutionnel de ces droits dans le prolongement de la jurisprudence développée et donner ainsi une assise plus ferme à ces droits lors de la balance avec des intérêts légitimes tels que la sécurité publique et la liberté d'entreprendre.

I. Introduction

La question du respect de la vie privée a radicalement changé de nature à l'ère digitale. Alors qu'il s'agissait d'un droit individuel à « être laissé tranquille »[1], cette conception mettant l'individu à l'abri de la société n'a plus de sens aujourd'hui pour des milliards d'usagers connectés en permanence, avides de partager leurs expériences sur les réseaux (presque 3 milliards de personnes sont actives sur les réseaux sociaux, soit 39% de la population mondiale). Le terme « numérique » serait en français plus conforme que celui de « digital » et donc recommandé, mais les termes sont polysémiques. Le mot « numérique » est plutôt lié à l'aspect technique alors que « digital » est en rapport avec l'usage des nouvelles technologies. Ces mots sont souvent utilisés de manière indifférente. La « bataille linguistique » étant un peu vaine, seul compte l'usage de la langue et seul le contexte d'usage permet de définir correctement les termes employés, si nécessaire celui-ci sera précisé dans ce rapport.

L'idée selon laquelle les droits de l'homme n'apparaissent pas tous au même moment est largement partagée et acceptée. Dans une perspective historique, les droits « naissent lorsque l'augmentation du pouvoir de l'homme sur l'homme qui suit inévitablement le progrès technique, c'est-à-dire la capacité de l'homme à dominer la nature et les autres hommes, crée soit de nouvelles menaces pour la liberté de l'individu soit consent des solutions nouvelles à son indigence... »[2]. Le processus historique n'est pas forcément linéaire de manière à conduire à plus de libertés. Mais force est de constater l'absence d'un *numerus clausus* des dangers qui menacent l'homme. Les droits dits nouveaux liés aux changements sociaux confirment l'inscription des droits dans une conception ouverte et évolutive. Cette conception rappelle qu'il faut sans cesse être attentif et ne jamais croire que les libertés (ni même la démocratie) soient acquises une fois pour toutes. Les nouvelles technologies sont le plus souvent perçues comme des menaces pour les libertés. Pour aborder les défis digitaux posés au respect de la vie privée, une brève évolution historique de la reconnaissance du droit à la vie privée est envisagée dans une perspective comparée.

I.1. Brève évolution historique de la reconnaissance du droit à la vie privée

Les spécialistes s'accordent à dater l'apparition de la vie privée entre les XVIIIe et XIXe siècles. Ces années ont été aussi déterminantes pour tracer la ligne de démarcation entre les sphères juridiques publique et privée de manière à reconnaître des droits limitant les pouvoirs de l'État. La bourgeoisie a rapidement demandé la reconnaissance d'un droit nouveau, mais indéfini, en vue de protéger sa vie privée de nouvelles menaces. En raison de l'urbanisation rapide, de la diffusion des caméras portables et de l'évolution des habitudes de lecture (en particulier, le développement de la presse à scandale), la société occidentale de plus en plus individualiste devenait plus sensible au besoin de préserver son intimité. Malgré des problèmes sociaux similaires, les juristes des traditions de *common law* et civiliste, perpétuant leur dichotomie historique, ont associé le droit nouveau à la vie privée à différents droits fondamentaux, respectivement : la liberté et la dignité. De nos jours, on voit encore cette fracture car les deux côtés de l'Atlantique semblent loin de trouver un terrain d'entente.

---

1 « The right to be let alone » : S.D. Warren, L.D. Brandeis, « The Right to Privacy », 4 *Harvard Law Review*, 1890, p. 193.

2 N. Bobbio, *L'età dei diritti*, Turin, Einaudi, 1992, p.XV.

Pourtant, non seulement l'opinion publique, mais aussi les juristes eux-mêmes croient que la vie privée, indépendamment de son nom (*privacy*, vie privée, *riservatezza*, *Privatsphäre* etc.), partage toujours le même sens, ou mieux, le même but. Beaucoup ont pensé ceci comme étant la conséquence de la transplantation de la conception juridique américaine de la vie privée à travers le monde. Ce n'est pas surprenant, puisque la plupart des universitaires considèrent le célèbre article de 1890 "The Right to Privacy", écrit par les avocats bostoniens Samuel Warren et Louis Brandeis dans la revue, *Yale Law Journal*, comme la pierre angulaire de la vie privée moderne. Néanmoins, il convient de noter que leur travail n'est pas sorti de nulle part, mais constitue plutôt la brillante synthèse et le développement des expériences à la fois anglaise et française, malencontreusement trop souvent négligées.

En effet, de nombreux éléments soutiennent la théorie d'une « double origine indépendante » de la vie privée, par opposition à la circulation, sinon à la transplantation, de l'expérience américaine. Cela explique pourquoi il a fallu plus de 70 ans aux États-Unis pour transposer l'idée doctrinale dans la jurisprudence de la Cour suprême. La première tourne autour de la notion de propriété et de liberté, tandis que la seconde est susceptible de provenir de la notion d'honneur développée sous l'Ancien Régime.

Pour rendre compte de ces origines différenciées, il convient avant tout de partir de l'expérience anglaise. Les juristes anglais ont associé la vie privée à la propriété, en la définissant comme le droit du propriétaire de s'opposer à toute ingérence étrangère sur son bien (*ius excludendi alios*). Néanmoins, la société anglaise a entamé un processus inexorable de « dématérialisation » des biens, en adoptant une régulation du droit d'auteur destinée à protéger la propriété contre des comportements sans rapport avec sa rétention matérielle. Par conséquent, la bourgeoisie a tenté de réguler la nouvelle « dimension intérieure » de la propriété (la vie privée à naître) en recourant aux mêmes *remedies* consacrés à la protection de sa nature physique et de son exploitation économique. Ce résultat a été facilité par le fait que les juges accordaient généralement des injonctions pour violation de contrat, violation du droit d'auteur, abus de confiance et *trespass*. Cependant, les tribunaux anglais ont fait face à de nombreuses difficultés tout en essayant de dépasser les limites de la propriété. En résumé, ils ont commencé à protéger les pensées, les sentiments et les émotions, à condition qu'ils s'exprimaient à travers les arts ou les écrits, en empêchant leur publication et leur diffusion quand ils n'étaient pas autorisés par le droit d'auteur. Les juges avaient clairement l'intention d'utiliser la propriété autrement que pour protéger un simple intérêt ou sentiment, pour prendre en compte un droit substantiel d'intérêt juridique. Enfin, lorsque le droit d'auteur a commencé à être insuffisant, ils ont entrepris d'accorder des injonctions pour la seule raison d'abus de *trust* ou de contrat. La dissociation entre les notions de propriété et de vie privée était la condition préalable nécessaire à la configuration ultérieure d'un droit individuel et autonome à être laissé tranquille.

La notion de « *privacy* » développée par Warren et Brandeis se rattache au contexte de *common law* mais elle ne pouvait pas s'appuyer sur les décisions des tribunaux anglais car ces dernières sont quasiment inexistantes[3]. Les avocats américains font en revanche référence à la loi française du 11 mai 1868 sur la presse alors même que des origines plus anciennes peuvent être décelées bien avant la Révolution de 1789.

Malgré une prise de conscience précoce de la vie privée (même si la notion est absente), déclenchée par de nombreux cas de diffamation dans les journaux, le législateur français a

[3] J.-L. Halpérin, "L'essor de la "privacy" et l'usage des concepts juridiques", *Droit et Société*, n° 61, 2005, p.770 : l'auteur précise qu'il y a toutefois une décision, *Prince Albert v. Strange* (1849) relative à la diffusion d'un catalogue des gravures du Prince Albert.

longtemps hésité à donner une définition claire de la vie privée, laissant ainsi son interprétation à la discrétion des tribunaux. En l'absence de code pénal, les auteurs de violations portant atteinte à l'ordre public ou à la réputation ont été sanctionnés sur la base de travaux académiques tels que le *Traité des injures* (1776) ou le *Répertoire universel* (1778). Au cours de l'Ancien Régime, une littérature abondante s'épanouit, inspirée par différents facteurs tels que les « causes célèbres », notamment la campagne de dénigrement contre la reine Marie-Antoinette.

Après la Révolution, la presse jouit d'une liberté illimitée (tous les crimes de presse ont été abrogés), ce qui entraîne de nombreux litiges civils relatifs à des écrits diffamatoires. « Dans un climat de suspicion à l'égard de la presse la plus révolutionnaire, accusée par de nombreux Constituants d'appeler à la désobéissance aux lois », Jean-Louis Halpérin a mis en lumière que « fut voté un article (inséré dans le chapitre V, titre III, article 17 de la Constitution de 1791) qui limitait les délits de presse à la provocation aux crimes et délits, à la calomnie volontaire contre les fonctionnaires publics et aux « calomnies et injures contre quelques personnes que ce soit relatives aux actions de leur vie privée » »[4]. Les constituants ont rejeté toute autre restriction à la liberté d'expression, à l'exception de la calomnie. La vérité, peu importe qu'elle soit regrettable ou désagréable, n'était pas considérée comme une menace pour l'intégrité des personnes.

En 1819, les trois lois "de Serre" – du nom du Garde des Sceaux de Louis XVIII – entendaient une fois de plus libéraliser la presse et distinguer pour la première fois entre la diffamation et l'insulte. Les lois de 1819, accompagnées du célèbre discours de Royer-Collard, développent l'idée que l'honneur et la réputation appartiennent à l'individu. Royer-Collard n'affirme-t-il pas : « il n'est pas permis de dire la vérité sur la vie privée » et d'ajouter : « voilà donc la vie privée murée, et si je puis me servir de cette expression, elle est déclarée invisible, elle est renfermée dans l'intérieur des maisons ». Ce n'est qu'en 1874 que la Cour de cassation a tenté de définir le contenu de la vie privée par un arrêt. La cour d'appel de Dijon avait condamné un journal pour avoir révélé le nom des participants (dont des parlementaires) à un pèlerinage à Notre-Dame d'Estang. L'arrêt étendait la notion de vie privée en dehors des murs domestiques, afin de couvrir tout ce qui relève du « domaine du for intérieur » ou de la « liberté de conscience ». Par la suite, la loi du 29 juillet 1881 sur la presse, malgré le fait qu'elle semblait avoir repris les mêmes principes que ceux des lois de 1819, aboutit finalement à la chute du « mur » entre les sphères publique et privée, permettant de regarder à travers. Cependant, cela ne s'appliquait qu'aux personnalités publiques en tant qu'artiste, politiciens, etc. Ce changement a ouvert la voie à une nouvelle évolution de la vie privée dans les années 1960, puis 70, afin de protéger également la vie privée des célébrités, dans la lignée de l'exemple américain.

Les expériences anglaise et française ont donc servi de tremplin sur lequel Warren et Brandeis se sont appuyés pour promouvoir un droit moderne visant à protéger les individus contre des intrusions indésirables dans leur vie privée. Leur article précité est incontournable puisqu'il représente le premier discours juridique reconnaissant le droit au respect de la vie privée comme un droit distinct. Dès que de nouveaux dispositifs et pratiques commerciales (en particulier, le développement de la photographie, de la publicité et de la presse "à sensation") ont commencé à menacer la personne de manière imprévue, la société américaine a elle aussi ressenti profondément le besoin d'obtenir ce que le juge Cooley définissait comme le droit à « être laissé tranquille »[5].

---

[4] J.-L. Halpérin « Protection de la vie privée et *privacy* : deux traditions juridiques différentes ? », *NCCC*, n°48, 2015, p. 61.

[5] L'idée est en effet empruntée au juge T.M. Cooley qui emploie pour la première fois la formule dans son ouvrage,

L'article de Warren et Brandeis ne montrait pas seulement qu'il y avait des atteintes à la vie privée sans lien avec la propriété et la diffamation, il suggérait aussi une nouvelle perspective juridique, où les valeurs personnelles étaient au-dessus des valeurs économiques. Il faudra quand même attendre 1905 pour que la Cour suprême de Géorgie, dans l'affaire *Paveish v. New England Life Insurance Company*, initie le mouvement favorable à la reconnaissance de la protection de la vie privée. Ce n'est donc que de manière progressive, affaire après affaire, que les juges ont façonné le droit des *torts* et sanctionné les atteintes à la vie privée. Mais comme toute évolution de *common law*, elle s'est faite à partir de l'existant : « Le droit au respect de la vie privée a reçu la protection de la *common law*, non pas en tant que tel, mais plutôt en tant qu'extension du droit naturel déjà protégé par elle, à savoir, le droit de propriété6 ». Cette construction judiciaire n'est toutefois pas sans faiblesse : lorsque l'individu n'est pas, ou n'est plus, propriétaire des éléments relatifs à sa vie privée (par exemple, les données détenues par une banque), il n'est plus protégé. Ainsi, la Cour suprême a jugé dans une affaire *United States v. Miller* (1976) que le droit à la vie privée ne pouvait plus être invoqué lorsque les éléments de la vie privée étaient entre les mains de tiers. C'est pourquoi les législateurs sont intervenus aux niveaux fédéral et fédéré pour compléter ce que la *common law* ne parvenait pas à protéger. Le droit à la vie privée présente deux facettes dans le droit constitutionnel américain : une dimension dite "passive" relative à la protection du secret des affaires personnelles et une dimension dite "active" relative à l'autonomie et au libre choix de la vie privée. Cette double dimension a été consacrée dans le célèbre arrêt de la Cour suprême de 1965, *Griswold v. Connecticut*.

En résumé, le régime de protection de la vie privée des États-Unis est caractérisé par une forte fragmentation : il comprend un dispositif législatif au niveau fédéral, de nombreuses autorités de surveillance, les constitutions des États et des lois spécifiques sur les données au niveau fédéré et, enfin, une interprétation judiciaire hétérogène. Il n'est pas surprenant qu'un système aussi complexe ait du mal à suivre le rythme de l'ère digitale.

I.2. Les défis posés par l'ère digitale au respect du droit à la vie privée

Bien que la vie privée soit un produit des siècles précédents, l'avènement de la société numérique a conduit sans surprise à lui faire subir un processus de reformulation, en passant du « droit à être laissé en paix » à la « protection des données personnelles ». La protection des données à caractère personnel constitue désormais l'une des dimensions du droit au respect de la vie privée. L'adoption rapide des nouvelles technologies de l'information par les organismes gouvernementaux et les entreprises a suscité la crainte que la surveillance secrète exercée par les États et les entités commerciales puisse avoir une incidence négative sur la vie privée et les libertés individuelles[7]. En même temps, il est de plus en plus évident que les mécanismes démocratiques sont affectés par les procédures dans lesquelles ces informations sont collectées et exploitées. L'ouverture des données publiques est ainsi présentée comme un enjeu à la fois économique et démocratique : économique d'abord car les données sont l'or

Treatise on the law of Torts or the Wrongs Which Arise Independently of Contract, (1878) publié par Callaghan & Company, 1907.

6 E. Zoller, « Le droit au respect à la vie privée aux États-Unis » in F. Sudre (dir.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruxelles, Bruylant, Coll. Droit et Justice n° 63, 2005, p. 39.

7 En 2013, le lanceur d'alerte Edward Snowden (sous-traitant pour la National Security Agency) révèle une surveillance planétaire pour le compte de l'agence de renseignements des États-Unis. Un programme, baptisé PRISM, a permis à la NSA et au FBI d'accéder aux données détenues par les géants de l'Internet (tels que Google, Yahoo…) et de consulter toute information relative à leurs utilisateurs.

noir du nouveau siècle[8] et aussi, démocratique car l'État lui-même n'hésite pas à mettre en avant un idéal de démocratisation de l'accès au droit par le numérique[9]. Antoine Garapon et Jean Lassègue ne s'y trompent pas en identifiant l'un des défis majeurs de cette révolution, souvent présentée comme la troisième révolution industrielle : « La révolution numérique est alimentée par le même vocabulaire de la démocratie qu'elle ne conteste pas mais qu'elle prétend au contraire porter à un niveau de réalité supérieur. D'où la difficulté de critiquer cette révolution, car le numérique prétend certes honorer les mêmes valeurs que le droit et la démocratie, mais tirant d'abord sa légitimité de lui-même, il peut tout aussi bien devenir l'instrument de leur trahison »[10].

Sans remettre en question la nécessité de sa protection et de son encadrement normatif, la vie privée continue d'avoir un contenu insaisissable qui entrave toute tentative de la définir de manière exhaustive. On observe simultanément que la protection de la vie privée et des données des individus est de plus en plus associée au droit à la dignité et à l'autodétermination de chaque être humain. Ces dernières semblent correspondre aux nouvelles valeurs fondamentales de la législation sur la protection des données.

Tous les aspects de la vie sociale sont saisis par ce processus global auquel la révolution numérique renvoie. En tout premier lieu, la sphère d'autonomie dont disposent les individus est bouleversée. D'un côté, le numérique est un nouvel espace de libertés[11]. En particulier, les libertés d'information et d'expression acquièrent une portée ignorée jusqu'alors puisque d'un seul 'clic', la communication peut être établie avec un nombre considérable de personnes. De l'autre, la numérisation est aussi constitutive d'un espace contre les libertés en donnant des possibilités de collecte, de stockage et d'exploitation des données personnelles sans commune mesure avec celles qui existaient auparavant (le *Big data* permettant une collecte massive des données sans finalité précise)[12]. Par exemple, en mettant à disposition du public (en "*open data*") l'ensemble des décisions de justice, un risque n'est-il pas pris à l'égard du respect des droits des tiers, notamment du droit à la vie privée des personnes concernées ?

Ces nouveaux risques liés à la datafication (autrement dit, la mise en données du monde) sont exposés de manière nettement plus large par un ancien président de la Commission Nationale Informatique et Libertés (CNIL, autorité de régulation créée par la loi Informatique et Libertés de 1978) : « Les caméras nous filment, les lecteurs biométriques nous identifient et nous reconnaissent, les dispositifs de géolocalisation nous repèrent et nous suivent, les applications Internet nous profilent, analysent nos goûts et enregistrent nos habitudes, les micros nous écoutent, l'arsenal des fichiers nationaux, européens et internationaux se déploie, le nuage numérique enveloppe la planète, l'informatique contextuelle comblera peu à peu les espaces disponibles entre nos pensées respectives, les nanotechnologies rendront les systèmes invisibles et donc innombrables et irréversibles (…). Si on ne réagit pas, la période durant

---

8 Pour la présidente de la CNIL, Isabelle Falque-Pierrotin, "les données privées sont le carburant du numérique" (*Le Monde*, 21 mai 2012).

9 En France, cela est ressorti de la nouvelle législation adoptée en 2016 visant à approfondir l'ouverture des données publiques et portant un intitulé pour le moins emphatique : loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (*JORF* du 8 octobre, texte n° 1).

10 A. Garapon, J. Lassègue, *Justice digitale*, Paris, PUF, 2018, p. 90.

11 Rapport du Conseil d'État, Le numérique et les droits fondamentaux, n° 64, 2014, pp. 145.

12 P. De Filippi, « Gouvernance algorithmique : vie privée et autonomie individuelle à l'ère des Big Data » in D. Bourcier et P. De Filipi (dir.), *Open Data & Big Data. Nouveaux défis pour la vie privée*, Paris, Mare & Martin, 2016, pp. 99.

laquelle la vie privée du citoyen, son intimité, son identité auront été reconnues et préservées n'aura été qu'une parenthèse »[13].

Si l'idée même de « vie privée » tend ainsi à perdre de sa force, de l'autre cette évolution reflète l'ambivalence de l'individu qui présente une double face. En effet, comme le souligne le rapport du Conseil d'État consacré à cette question, le lien entre le droit à la vie privée et le numérique est fréquemment envisagé sous l'angle unique des atteintes du second au premier. Il est vrai qu'en plein scandale Cambridge Analytica, les géants de l'internet (les GAFAM : Google, Apple, Facebook, Amazon, Microsoft) ne peuvent pas échapper à la suspicion[14]. Cependant, les réseaux permettent également de rendre plus effectif un autre aspect du droit à la vie privée entendu comme « le droit pour l'individu de nouer et de développer des relations avec ses semblables » (Cour EDH, 16 décembre 1992, *Niemetz c. Allemagne*, n° 13710/88)[15]. Il est désormais traditionnel de mettre en évidence ce "paradoxe de la vie privée" très souvent évoqué dans les travaux académiques anglo-américains (*privacy paradox*) : se montrer, notamment sur les réseaux sociaux, pour avoir une vie publique. Cette ambivalence a pour conséquence de détendre le rapport entre vie privée et donnée personnelle : autrement dit, il n'y a plus de frontière nette entre vie privée et vie publique et donc de nouvelles perspectives de protection des droits doivent être envisagées[16].

Dans le contexte français, cette recherche est actuellement très intense. D'un côté, les avancées de la législation européenne avec le Règlement général sur la protection des données (RGPD) et de l'autre, la future révision constitutionnelle sont des moteurs de réflexion alors que la France s'était dotée en 1978 d'un dispositif législatif novateur avec la loi Informatique et Liberté[17]. La Commission consultative nationale des droits de l'homme (CNCDH) s'est autosaisie de ces enjeux et a rendu un avis le 22 mai 2018 intitulé « Protection de la vie privée à l'ère numérique »[18]. C'est le sens même de la notion de vie privée qui est questionnée dans l'espace numérique. Cela induit sur le plan juridique que soit discutée l'idée suivante[19] : doit-on introduire dans la Constitution de 1958 de nouveaux droits pour faire face aux défis digitaux ? Toutefois, l'éventuelle introduction dans la Constitution de droits nouveaux n'épuise pas le débat car la question de fond est avant tout de savoir si l'on veut accroître la capacité d'action des individus en leur donnant un droit de regard sur le traitement de leurs données

---

13 A. Türk, *La vie privée en péril*, Paris, Odile Jacob, 2011, p. 261.

14 Facebook est accusé d'avoir permis au cabinet Cambridge Analytica de mettre la main de manière détournée sur les données de 87 millions d'internautes pendant la dernière campagne présidentielle américaine. YouTube, filiale de Google, a été visée en avril 2018 par une plainte collective de 23 associations américaines de défense des droits numériques et de protection de l'enfance. YouTube, officiellement interdit aux moins de 13 ans, est accusé d'avoir collecté des informations personnelles sur les mineurs (géolocalisation, numéros de portables...) pour réaliser du ciblage publicitaire et sans en informer les parents.

15 Rapport du Conseil d'État précité, p.146.

16 Rapport du Conseil d'État précité, pp.153.

17 La loi de 1978 est une réaction du parlement au projet de fichier SAFARI (acronyme de « Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus ») qui visait à centraliser des bases de données de l'ensemble des services de police grâce à un ordinateur de nouvelle génération.

18 Avis de la CNCDH, *JORF* du 3 juin 2018 (texte n° 6). Au cours de ces dernières années, maints rapports produits par différentes institutions peuvent être cités dont l'importante étude annuelle du Conseil d'État sur les droits fondamentaux et le numérique, précitée.

19 Dans le cadre de la révision constitutionnelle engagée depuis mai 2018, a été constitué à l'initiative des Présidents des assemblées un groupe de travail sur les droits et libertés constitutionnels à l'ère numérique coprésidé par un sénateur (C.-A. Frassa) et une députée (P. Forteza) pour réfléchir à la rédaction d'une charte constitutionnelle du numérique (à l'instar de la Charte de l'environnement adossée au préambule de la Constitution de 1958).

personnelles. Jusqu'à présent, il s'agit pour l'essentiel de droits permettant aux individus de rester à l'écart du traitement de leurs données. Au-delà de la question du niveau de protection (constitutionnel ou législatif), c'est donc bien un changement de logique qui est en jeu en encourageant « l'autonomisation » ou mieux l'*empowerment* des individus face aux défis digitaux[20].

[20] Ce changement de logique est souligné dans le rapport du Conseil d'État précité, en particulier, pp. 262.

II. La notion de droit au respect de la vie privée dans la législation française

II.1. L'absence d'une reconnaissance explicite par la constitution

À la différence de certaines constitutions (comme par exemple l'article 22 de la Constitution belge modifiée en 1994), la Constitution française ne reconnaît pas expressément un droit au respect de la vie privée. Le texte fondamental ne protège pas en tant que tel ce droit qui a été reconnu progressivement par le Conseil constitutionnel (voir la partie suivante). De même, ni les avancées de l'informatique, ni celles du numérique, n'ont conduit jusqu'à présent à une inscription dans le préambule de la Constitution de 1958 reconnaissant à toute personne « le droit d'être protégée contre l'emploi abusif des données qui la concernent » (tel est ainsi formulé ce droit à l'article 13 de la Constitution suisse de 1999). À l'ère de « la société d'information » et des risques d'abus qui en résultent, la question d'un ancrage constitutionnel se pose dans le contexte français où le législateur ordinaire est intervenu en revanche à plusieurs reprises pour garantir des droits aux individus face aux intrusions dans leur vie privée.

II.2. La reconnaissance législative d'un droit gigogne

Depuis les années 1970, le législateur a adopté plusieurs lois visant à assurer des garanties aux individus face aux intrusions de plus en plus nombreuses dans leur vie privée. Le législateur a plutôt réagi face à des dangers nouveaux sans chercher à construire un dispositif cohérent. Par conséquent, l'arsenal législatif existant repose sur plusieurs droits qui s'emboîtent plus ou moins dans le droit au respect de la vie privée qui apparaît comme le droit premier à partir duquel plusieurs droits se déclinent notamment la protection des données personnelles.

II.2.1. Le droit au respect de la vie privée *stricto sensu*

La notion juridique apparaît plutôt tardivement en France puisqu'il faut attendre la loi du 17 juillet 1970 pour voir consacré dans le Code civil le principe selon lequel « chacun a droit au respect de sa vie privée » (article 9 alinéa 1). Cette loi est intervenue après que plusieurs textes internationaux et européens aient reconnu un droit subjectif (article 12 de la Déclaration universelle des droits de l'homme, article 12 du Pacte international relatif aux droits civils et politiques, article 8 de la Convention européenne des droits de l'homme)[21]. L'alinéa 2 de l'article 9 du Code civil prévoit une protection renforcée en cas d' "atteinte à l'intimité de la vie privée".

En l'absence de définition légale de son contenu, ce droit est susceptible de s'adapter aux évolutions mentales, pratiques et technologiques de la société. Il présente traditionnellement trois aspects que les juges ont discernés au fil des affaires : inviolabilité du domicile, libre choix de la vie privée et secret de la vie privée. Dans le cadre de ce dernier volet, la protection des données personnelles s'est développée avec la généralisation de l'informatique et la multiplication des possibilités de stockage des données. La première composante peut être intégrée dans le troisième aspect. Ainsi, est-il possible d'identifier les deux aspects centraux du droit au respect de la vie privée[22] : un droit « interne » de préserver sa sphère d'intimité des

[21] Le contexte juridique international a sans doute eu son importance. Néanmoins, comme souvent, c'est une affaire qui a fait réagir le législateur en 1970 : une scandaleuse campagne de presse contre le Président de la République de l'époque.

[22] Les ouvrages français consacrés aux droits de l'homme et aux libertés publiques sont partagés sur la

intrusions extérieures, et un droit « externe » de déployer librement sa personnalité dans la vie sociale, notamment en communiquant ses informations personnelles selon sa convenance.

Dans une perspective classique et large, la vie privée correspond à la « *sphère secrète de la vie d'où [l'individu] aura le pouvoir d'écarter les tiers* »[23]. Ainsi conçu, ce droit permet d'abord de s'opposer à toute intrusion non consentie dans sa sphère intime. Le droit au respect de la vie privée est donc un « droit de se voiler ou de se masquer » qui vaut pour tout individu, dans toutes les sphères de la vie sociale, y compris dans les relations de travail. La protection de l'intimité de la personne porte à la fois sur l'ensemble des éléments matériels (son patrimoine, son domicile, ses correspondances) et immatériels de la vie d'une personne (son image, son corps, sa vie amoureuse et spirituelle).

En particulier, l'objectif de lutte contre le terrorisme et la délinquance organisée n'a cessé de fragiliser le secret des communications privées. Le développement des technologies menace d'anéantir ce secret par le déploiement d'une surveillance potentiellement généralisée : ce qui a conduit le législateur à définir les garanties légales portant sur les motifs susceptibles de justifier la surveillance. Tel est l'objectif de la loi du 24 juillet 2015 relative au renseignement.

L'article L.801-1 du Code de la sécurité intérieure rappelle que « le secret de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données personnelles et l'inviolabilité du domicile, est garanti par la loi. L'autorité publique ne peut y porter atteinte que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci dans le respect du principe de proportionnalité ». À cette fin, une nouvelle autorité administrative indépendante, la Commission nationale des techniques de renseignement (CNCTR) a été créée : elle est chargée, avec le Conseil d'État, d'assurer le respect de ces principes. Le recours aux techniques de renseignement est justifié par de nombreux intérêts fondamentaux : l'indépendance nationale, l'intégrité du territoire, la défense nationale, la prévention du terrorisme, la lutte contre la criminalité et la délinquance organisée, et les intérêts économiques et scientifiques majeurs de la France.

Les atteintes à la vie privée peuvent aussi se concrétiser en dehors de ces hypothèses liées aux exigences de sécurité publique lors d'une utilisation habituelle d'Internet, notamment par la fréquentation des réseaux sociaux sur lesquels des renseignements les plus intimes peuvent être dévoilés ou bien en utilisant les publicités ciblées. La directive ePrivacy 2002/58 du 11 juillet 2002 (également appelée « Directive cookie ») a été transposée en France par l'ordonnance dite « Paquet Telecom » (ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques). Cette transposition est importante puisque désormais les internautes doivent en principe donner leur accord préalablement à l'inscription de cookies (article 32 de la loi de 1978).

On observera pour conclure que la doctrine privatiste s'interroge en particulier sur l'introduction de ce droit parmi les droits de la personnalité même si certains prônent le singulier en s'appuyant sur l'exemple allemand[24] : l'article 2 de la Loi fondamentale prévoit que « [c]hacun a droit au libre développement de sa personnalité, pourvu qu'il ne porte pas atteinte aux droits d'autrui, à l'ordre constitutionnel ou à la loi morale ». Quoi qu'il en soit, les reconstructions doctrinales montrent toutes que le droit au respect de la vie privée est un droit

---

décomposition des aspects du droit à la vie privée. Voir S. Hennette-Vauchez et D. Roman, *Droits l'homme et libertés fondamentales*, Paris, Dalloz, 3e éd., 2017, pp. 515 : les auteurs distinguent ainsi le « droit de se voiler » du « droit de se dévoiler ».

23 J. Carbonnier, *Droit civil*, vol.1, Paris, P.U.F., 2004, p. 518.

24 Voir J. Antippas et B. Beignier, « La protection de la vie privée » in R. Cabrillac (dir.), *Libertés et droits fondamentaux*, Paris, Dalloz, 24e éd., 2018, p. 225.

fondamental ; elles se divisent en revanche sur les démembrements de ce droit, mais en s'accordant sur l'importance prise par le droit à la protection des données personnelles. En ce sens, la reconnaissance autonome de ce droit à côté de celui au respect de la vie privée par la Charte des droits fondamentaux de l'Union européenne (articles 7 et 8) est systématiquement rappelée.

II.2.2. Le droit à la protection des données personnelles et ses prolongements

La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ou la loi « Informatique et Libertés ») a mis en place un dispositif pionnier pour faire face aux risques que comporte la prolifération des données. Ce dispositif se fonde sur le principe que « toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés » (article 3) et sur les pouvoirs confiés à une autorité administrative indépendante, la Commission nationale de l'informatique et des libertés (CNIL).

La prospérité de cette loi repose sur l'identification novatrice des enjeux de l'informatique dont son article 1er témoigne : « L'informatique doit être au service de chaque citoyen. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». Elle repose aussi sur son adaptation à la fois aux exigences européennes et aux avancées technologiques.

Au début des années 1990, les instances européennes se sont saisies de cette question. Le développement des échanges intracommunautaires, alors même que plusieurs États membres n'étaient dotés d'aucune législation comparable à la loi "Informatique et Libertés" ou bien dotés de textes, qui s'ils visaient le même objectif de protection des individus, procédaient toutefois de traditions juridiques différentes et instauraient des procédures variées, a conduit à intervenir afin d'harmoniser les dispositifs de protection des données. Ainsi, a été adoptée la directive 95/46 du 24 octobre 1995 visant à créer les conditions d'une libre circulation des données à caractère personnel entre les États membres, en garantissant un seuil minimal de protection de la vie privée dans tout l'espace de l'Union. Le choix communautaire reposait toutefois sur une logique inverse de celle adoptée dans la loi de 1978 : autrement dit, la directive a favorisé le contrôle *a posteriori* au détriment du contrôle *a priori* de conformité des traitements à la loi par l'autorité indépendante chargée du contrôle.

Le dispositif de la loi de 1978 a été complétement refondu pour tenir compte des exigences communautaires par la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Le contrôle *a priori* a été maintenu en 2004 pour les traitements portant sur les données sensibles (données génétiques, origines raciales ou ethniques, opinions et croyances, appréciations sur les difficultés sociales des personnes, données relatives à la commission d'infractions…). Une donnée à caractère personnel n'est pas nécessairement un élément de la vie privée. Le nom patronymique, par exemple, ne relève pas de la vie privée. Selon l'article 2 de la loi de 1978, une donnée à caractère personnel est constituée par « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ».

Avant même l'application du RGPD, la France a fait le choix d'affirmer ses positions dans un texte de loi intitulé de manière emphatique « Pour une République numérique »[25]. Ce texte comporte un volet relatif à la protection des droits dans la société numérique qui vient compléter la loi de 1978 en consacrant pour la première fois le droit de disposer librement de ses données.

L'article 1er de la loi de 1978 est ainsi complété : « toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant ». Les individus deviennent ainsi les premiers artisans de la protection de leur vie privée. Le renforcement de la maîtrise des données suppose de consolider les droits personnels et donc la capacité des individus à décider de la diffusion et de l'utilisation de leurs données personnelles. Cet ajout peut être interprété comme un premier pas vers la reconnaissance d'un droit à l'autodétermination informationnelle souvent évoqué au sein de la doctrine française dans le prolongement de la jurisprudence constitutionnelle allemande (1983) et le rapport annuel du Conseil d'État (2014).

À la suite de la jurisprudence européenne relative au droit au déréférencement (CJUE 13 Mai 2014 *Google Spain*), le droit à l'effacement a été renforcé pour les personnes mineures par la mise en place d'une procédure accélérée : le responsable du traitement est tenu d'effacer dans les meilleurs délais les données collectées lorsque la personne à l'origine de la demande était mineure au moment de leur communication. En cas d'inaction, la CNIL peut être saisie dans un délai d'un mois et doit se prononcer dans un délai de trois semaines. Des limites à ce droit à l'effacement des données collectées licitement sont fixées : lorsque le traitement est nécessaire pour exercer la liberté d'expression et le droit à l'information ; pour des motifs d'intérêt public ; ou pour respecter une obligation légale (art. 40 II (nouveau) de la loi de 1978). Cette intervention législative alors que le RGPD était en cours d'adoption, a été critiquée par le Conseil d'État jugeant cette transposition « partielle et approximative, tant [s'agissant] de la définition des données concernées par ce droit, que l'étendue de ce droit »[26].

Le législateur français à la différence du RGPD a décidé de prévoir des règles relatives au traitement des données personnelles des personnes décédées en reconnaissant un droit à la maîtrise de ses données *post-mortem*. Dans le prolongement du droit de disposer librement de ses données posé au nouvel article 1er de la loi de 1978, l'article 40-1 prévoit un droit nouveau pour toute personne concernée de définir des « directives relatives à la conversation, à l'effacement et à la communication de ses données à caractère personnel après son décès ». Le dispositif mis en place est qualifié de « testament numérique »[27].

Enfin, le législateur a poursuivi le renforcement de la logique de la maîtrise des données en insérant un nouvel article au code des postes et des communications électroniques : l'article L 32-3 prévoit que « les opérateurs, ainsi que les membres de leur personnel, sont tenus de respecter le secret des correspondances". Le secret des correspondances électroniques des internautes couvre l'identité des correspondants, l'intitulé, les documents joints et le contenu des mails. Les traitements automatisés d'analyse des mails à des fins publicitaires, statistiques ou d'amélioration du service apporté aux utilisateurs sont interdits, à moins que ces derniers y consentent expressément (consentement à renouveler au moins une fois par an).

---

25 Loi du 7 octobre 2016 précitée.

26 Avis consultatif du CE n° 390741, République numérique, point 40.

27 Voir L. Cluzel-Métayer, « La loi pour une République numérique : l'écosystème de la donnée saisi par le droit », *AJDA* 2017, p.343.

Enfin, la loi pour une République numérique a repris les principes européens qui s'appliquent aux acteurs du numérique dans un environnement ouvert en vue de renforcer des pratiques transparentes : neutralité de l'internet et loyauté des plateformes.

Par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles[28], l'adaptation de la loi de 1978 au RGPD a été parachevée. Cette loi n'est pas une transposition du RGPD, mais de la directive 2016/680 dite "directive police". Le législateur a toutefois profité des espaces de liberté laissés aux États membres de manière à adapter la loi de 1978 qui est donc toujours en vigueur. Cela a conduit à faire disparaître les formalités préalables à la création des traitements. Désormais, le système de protection repose sur l'appréciation des risques par le responsable du traitement lui-même, la CNIL exerçant un contrôle *a posteriori*. Il convient de souligner que les pouvoirs de la CNIL ont été renforcés notamment ceux de sanction. Elle a aussi désormais un rôle de certification et de conseil puisqu'elle peut être consultée par le Parlement sur les questions de protection des données personnelles. Le Conseil constitutionnel a validé le nouveau dispositif (décision 2018-765 DC, voir la section suivante).

[28] *JORF*, 21 juin 2018, texte n° 1.

III. Jurisprudence la plus pertinente en la matière

III.1. Éléments introductifs sur la jurisprudence constitutionnelle

Comme souligné précédemment, la Constitution de 1958 ne reconnaît expressément ni le droit au respect de la vie privée, ni le droit à la protection des données personnelles. Ces droits ont été consacrés de manière progressive selon un cheminement qui peut paraître sinueux[29]. Faute d'une base textuelle expresse, le Conseil constitutionnel a tâtonné avant de reconnaître le droit au respect de la vie privée comme droit fondamental, puis de lui rattacher le droit à la protection des données personnelles.

Le droit à la vie privée est déduit de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 auquel renvoie le préambule de la Constitution et le droit à la protection des données personnelles est lui-même déduit du droit à la vie privée. Ce dernier droit est un prolongement du premier et ne semble pas être autonome par rapport à celui-ci[30].

La jurisprudence française semble en retrait par rapport aux jurisprudences constitutionnelles des cours voisines, notamment allemande (voir la conclusion de ce rapport). C'est "davantage le *secret* que la *liberté* de la vie privée qui s'y trouve garantie"[31].

III.2. La reconnaissance constitutionnelle du droit au respect de la vie privée

III.2.1. Décision n° 94-352 DC du 18 janvier 1995 – *Loi d'orientation et de programmation relative à la sécurité* (décision dite « vidéosurveillance »)

À la différence de la décision 76-75 DC du 12 janvier 1977 dite « fouille des véhicules » dans laquelle le Conseil constitutionnel adoptait une conception large de la liberté individuelle, y incluant le droit au respect de la vie privée, il reconnait dans cette décision de 1995 explicitement le droit au respect de la vie privée sur le fondement de la liberté individuelle mentionnée à l'article 66 alinéa 2 de la Constitution (« L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi »).

Appelé à se prononcer sur la constitutionnalité de dispositions encadrant l'installation de systèmes de vidéosurveillance, le Conseil a jugé « que la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle ».

---

29 Nous avons décidé de ne retracer que partiellement ce parcours sinueux puisque depuis 1999, la jurisprudence semble stabilisée. Pour plus de détails, voir P. Wachsmann, *Libertés publiques*, Paris, Dalloz, 8e éd., 2017, pp. 207.

30 La protection des données personnelles comme composante du droit au respect de la vie privée correspond également au positionnement de la CEDH laquelle prend acte que la Convention de sauvegarde ne consacre pas d'article spécifique à ce droit et donc fait découler celui-ci de l'article 8 relatif au droit à la vie privée : CourEDH, Grande chambre, 4 décembre 2008, *S. et Marper c. Royaume-Uni*, n° 30562/04 et 30566/04. En revanche, les droits au respect de la vie privée et à la protection des données personnelles bénéficient d'une reconnaissance propre dans la Charte des droits fondamentaux de l'Union européenne.

31 V. Mazeaud, « La constitutionnalisation du droit au respect de la vie privée », *NCCC*, 2017, n° 48, p.17 (souligné par l'auteur).

III.2.2. Décision n° 99-416 DC du 23 juillet 1999 – *Loi portant création d'une couverture maladie universelle*

Le Conseil constitutionnel consacre le droit au respect de la vie privée comme droit autonome qui n'est plus un aspect de la liberté individuelle à l'occasion du contrôle des dispositions mettant en place les cartes comprenant les données relatives aux assurés sociaux.

Le Conseil rattache le droit à la protection de la vie privée à l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789. La vie privée se déduit désormais de « la liberté » reconnue à l'article 2 qui dispose que « le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression ».

Par ailleurs, le Conseil reconnaît la compétence du législateur pour fixer le cadre juridique en matière de données personnelles. Il précise qu'il appartient au législateur « d'instituer une procédure propre à sauvegarder le respect de la vie privée des personnes, lorsqu'est demandée la communication de données de santé susceptibles de permettre l'identification de ces personnes ».

III.2.3. Décision 2004-492 DC du 2 mars 2004 – *Loi portant adaptation de la justice aux évolutions de la criminalité*

Dans cette décision, le Conseil rappelle au législateur ses obligations à savoir "assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des libertés constitutionnellement garanties".

Il précise "qu'au nombre de celles-ci figurent la liberté d'aller et venir, l'inviolabilité du domicile privé, le secret des correspondances et le respect de la vie privée, protégés par les articles 2 et 4 de la Déclaration de 1789, ainsi que la liberté individuelle, que l'article 66 de la Constitution place sous la surveillance de l'autorité judiciaire". Ce qui sera rappelé dans sa décision sur la loi relative au renseignement (décision 2015-713 DC, ci-dessous).

On observera par ailleurs que le Conseil consacre les trois composantes traditionnelles de la vie privée dans cette décision (inviolabilité du domicile privé, secret des correspondances et respect de la vie privée). Il semble les distinguer. Les difficultés des reconstructions doctrinales évoquées précédemment viennent précisément d'une jurisprudence constitutionnelle au caractère fluctuant et aux fondements conceptuels incertains.

III.3. Modalités du contrôle exercé sur le respect du droit à la vie privée

III.3.1. Décision n° 94-352 DC du 18 janvier 1995 – *Loi d'orientation et de programmation relative à la sécurité* (décision dite « vidéosurveillance »)

Le Conseil constitutionnel a tenu à préciser que le droit ouvert à toute personne intéressée de s'adresser au responsable d'un système de vidéosurveillance afin d'obtenir un accès aux enregistrements qui la concernent, que l'on peut concevoir comme une garantie du droit au respect de la vie privée, pouvait être refusé dans l'hypothèse où une telle communication serait de nature à porter atteinte au secret de la vie privée de tiers. Ainsi, le juge constitutionnel est-il attentif à ce que certains dispositifs publics actionnés par des personnes privées ne constituent pas des atteintes indirectes aux droits des tiers.

III.3.2. Décision n° 2004-504 DC du 12 août 2004 – *Loi relative à l'assurance maladie*

Le Conseil constitutionnel exerce un contrôle de proportionnalité s'agissant du droit au respect de la vie privée et donc du droit à la protection des données personnelles. Ce contrôle de proportionnalité exercé à plusieurs reprises par le Conseil constitutionnel se limite à la vérification qu'aucune erreur manifeste n'a été commise (décision du 26 janvier 2017 DC 2016-745 ; rappel dans sa récente décision du 12 juin 2018 relative à la loi sur la protection des données personnelles, voir ci-dessous)

III.3.3. Décision n° 2010-25 QPC du 16 septembre 2010 – *M. Jean-Victor C.* [Fichier empreintes génétiques]

Le droit au respect de la vie privée devient un droit invocable dans le cadre d'une question prioritaire de constitutionnalité (QPC).

Le Conseil estime que l'inscription au fichier national automatisé des empreintes génétiques des personnes non condamnées, mais à l'égard desquelles il existe certains indices de leur participation aux infractions en cause, assure une conciliation équilibrée entre la sauvegarde de l'ordre public et le respect de la vie privée. Pour résumer, le Conseil juge le risque pour les libertés de conserver les traces d'une infraction peut-être commise, moins grave que celui de ne pas retrouver l'information si le suspect est en effet l'auteur de l'infraction. L'intervention du juge judiciaire est exigée.

III.3.4. Décision n° 2015-713 DC du 23 juillet 2015 – *Loi sur le renseignement*

Les auteurs de la saisine contestaient ce texte de loi en ce qu'il ne présentait pas de garanties suffisantes au regard des droits et libertés constitutionnels et ils contestaient particulièrement le fait que le recours aux techniques de renseignement n'était pas placé sous le contrôle du juge judiciaire en méconnaissance de l'article 66 de la Constitution. Le Conseil a pourtant considéré que « le recueil de renseignements au moyen des techniques définies au titre V du livre VIII du code de la sécurité intérieure par les services spécialisés de renseignement pour l'exercice de leurs missions respectives rele[vait] de la seule police administrative ». Les juges constitutionnels ont donc appliqué un syllogisme imparable : la finalité du renseignement est la préservation de l'ordre public ; il relève donc du champ de la police administrative ; autorités administratives et juge administratif sont donc compétents.

Il faut souligner que l'action des services de renseignement, à la différence des missions classiques de police, peut porter sur des informations personnelles qui n'ont qu'une utilité éventuelle et non certaine au moment de leur collecte. Malgré le grief des députés soutenant un risque d'atteinte disproportionnée à la vie privée en raison du nombre de données susceptibles d'être contrôlées, le Conseil constitutionnel a validé la disposition du fait de l'existence de certaines garanties procédurales, notamment l'avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR) et une autorisation délivrée pour une durée limitée.

III.3.5. Décision n° 2015-722 DC du 26 novembre 2015 – *Loi relative aux mesures de surveillance des communications électroniques internationales*

Le texte de loi soumis à l'examen du Conseil légalise la pratique de la surveillance non individualisée de « groupes de personnes », d'organisations et même de zones géographiques. Ce dispositif a été jugé conforme à la Constitution ainsi que le traitement assoupli des données de connexion. Pour le juge constitutionnel, l'ensemble des dispositions examinées « ne portent

pas d'atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances » (cons. 15).

III.3.6. Décision n° 2016-590 QPC du 21 octobre 2016 – *La Quadrature du Net et autres* [Surveillance et contrôle des transmissions empruntant la voie hertzienne]

Le Conseil constitutionnel a censuré l'article L. 811-5 du code de la sécurité intérieure qui excluait toutes les ondes hertziennes (Wi-Fi, téléphonie mobile…) des mécanismes de protection de la vie privée et du droit au secret des correspondances.

Passé inaperçu lors des débats sur la loi Renseignement, l'article L. 811-5 du code de la sécurité intérieure venait discrètement offrir une voie royale pour les services qui souhaitaient pouvoir continuer à écouter les réseaux télécoms sans aucune restriction ni aucun contrôle par qui que ce soit, dès lors que les communications interceptées utilisent à un moment ou un autre des ondes hertziennes (ce qui est le cas notamment de la téléphonie mobile, du Wi-Fi, de la téléphonie fixe lorsqu'elle passe par des téléphones sans fil, du Bluetooth, du NFC…).

Le Conseil constitutionnel a censuré une surveillance sans « aucune condition de fond ni de procédure », et sans « aucune garantie » dans sa mise en œuvre. Il constate que la seule condition de la « défense des intérêts nationaux » posée à la mise en œuvre de la surveillance hertzienne ne vaut rien puisque, ensuite, rien n'interdit ni n'empêche « que ces mesures puissent être utilisées à des fins plus larges ».

III.3.7. Décision 2018-696 QPC du 30 mars 2018 – *M. Malek B.* [Pénalisation du refus de remettre aux autorités judiciaires la convention secrète de déchiffrement d'un moyen de cryptologie]

La pénalisation du refus de remettre une clé de déchiffrement susceptible d'avoir été utilisée pour commettre une infraction est conforme à la Constitution, plus particulièrement au droit au respect de la vie privée protégé par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789.

III.4. La reconnaissance du droit à la protection des données personnelles

III.4.1. Décision n° 92-316 DC du 20 janvier 1993 – *Loi relative à la prévention de la corruption et à la transparence de la vie économique et des procédures publique*

Le Conseil constitutionnel semble, pour la première fois, donner valeur constitutionnelle au droit à la protection des données personnelles selon laquelle la loi « Informatique et libertés » participe de la protection de la liberté individuelle. En l'espèce, le Conseil constitutionnel ne rattache pas la protection constitutionnelle contre le traitement abusif des données à caractère personnel à la protection du droit au respect de la vie privée.

Le Conseil insiste sur le fait que le législateur n'a pas entendu déroger aux dispositions protectrices de la liberté individuelle prévues dans la législation relative à l'informatique, aux fichiers et aux libertés (cons. 14). Ce qui signifie que le législateur devra être prudent lorsqu'un texte législatif comportera des dispositions affectant la liberté individuelle par le biais du fichage et du traitement automatisé de données personnelles. Au regard de la nature

constitutionnelle de la liberté en cause, le législateur devra assurer un degré de protection suffisant.

La doctrine s'est un temps demandée si la loi du 6 janvier 1978 n'avait pas elle-même valeur supra-législative au regard de cette jurisprudence faisant de la loi une garantie de la liberté individuelle.

III.4.2. Décision n° 93-325 DC du 13 août 1993 – *Loi relative à la maîtrise de l'immigration et aux conditions d'entrée, d'accueil et de séjour des étrangers en France*

De nouveau, le Conseil constitutionnel considère la loi du 6 janvier 1978 comme une garantie procédurale du droit à la protection des données personnelles. Le Conseil a ainsi pu décider que le législateur avait « explicitement entendu assurer l'application des dispositions protectrices de la liberté individuelle prévues par la législation relative à l'informatique, aux fichiers et aux libertés ».

III.4.3. Décision n° 2003-467 DC du 13 mars 2003 – *Loi pour la sécurité intérieure*

Cette décision est intéressante lorsqu'on en vient à s'interroger sur le fondement du droit à la protection des données personnelles. Ce droit, d'ailleurs innomé par le Conseil constitutionnel, est rattaché au droit au respect de la vie privée. Mais au-delà du droit au respect de la vie privée, le droit à la protection des données personnelles conditionne l'exercice de nombreux droits.

Dans son considérant 32, le Conseil fait un lien entre identification et données personnelles. Il reconnait peut-être par là le lien entre identité et protection des données personnelles. Néanmoins, le droit constitutionnel français demeure sur la réserve en matière d'identité.

III.4.4. Décision n° 2004-499 DC du 29 juillet 2004 – *Loi 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*

Le Conseil constitutionnel rattache le droit à la protection des données personnelles à la protection de la vie privée.

Le Conseil a jugé que les traitements techniques mis en œuvre par les opérateurs de télécommunication ne pouvaient, sous peine de contrevenir au droit au respect de la vie privée, acquérir un caractère nominatif que dans le cadre d'une procédure judiciaire. Le droit à la protection des données personnelles dans la jurisprudence du Conseil constitutionnel n'est en effet qu'une implication du droit au respect de la vie privée, lui-même rattaché à l'article 2 de la Déclaration des droits de l'homme et du citoyen qui fait figurer la liberté parmi les « droits naturels et imprescriptibles de l'Homme ».

Cette liaison du droit au respect de la vie privée, et par ricochet, du droit à la protection des données personnelles, à l'article 2 de la Déclaration de 1789, exprime la réalité de l'attachement du Conseil constitutionnel au texte de la Constitution.

III.4.5. Décision n° 2018-765 DC du 12 juin 2018 – *Loi relative à la protection des données personnelles*

Dans cette récente décision, le Conseil rappelle à l'occasion de l'examen de la loi adaptant la loi « informatique et Libertés » de 1978 aux dispositions du RGPD lui-même entré en application le 25 mai 2018 que « la liberté proclamée par l'article 2 de la Déclaration de 1789 implique le droit au respect de la vie privée. Par suite, la collecte, l'enregistrement, la

conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif ».

Par cette décision, le Conseil confirme donc le rattachement de la protection des données personnelles au respect de la vie privée (la décision n° 2004-499 DC précitée) sans lui donner un fondement autonome.

III.5. Modalités du contrôle exercé pour assurer le respect du droit à la protection des données personnelles

III.5.1. Décision n° 2004-492 DC du 2 mars 2004 – *Loi portant adaptation de la justice aux évolutions de la criminalité*

Le Conseil constitutionnel exerce un contrôle normal sur la possibilité de consultation par des autorités administratives du fichier automatisé des auteurs d'infractions sexuelles. Il passe d'un contrôle restreint à un contrôle normal. Par ailleurs, le Conseil reconnait la compétence du juge judiciaire en matière de données personnelles.

III.5.2. Décision n° 2009-580 DC du 10 juin 2009 – *Loi favorisant la diffusion et la protection de la création sur internet*

Dans cette décision, une disposition de loi prévoyait une dérogation au principe d'interdiction des fichiers privés d'infractions au profit des « personnes morales victimes d'infractions ou agissant pour le compte desdites victimes pour les besoins de la prévention et de la lutte contre la fraude ». À l'origine, la loi du 6 janvier 1978 avait une approche restrictive de la liste des personnes morales susceptibles de créer des fichiers d'infractions, en dehors des personnes publiques habilitées. La disposition contestée, qui créait une nouvelle catégorie de personnes autorisées à créer des fichiers d'infractions, fut censurée par le Conseil constitutionnel pour incompétence négative.

Selon le Conseil constitutionnel, il faut que le législateur définisse de manière précise les modalités d'application de ces traitements tant ils sont dangereux compte tenu de leur ampleur et de la nature des informations traitées (infractions, condamnations, mesures de sûreté). La loi, se contentant d'évoquer la fraude pour justifier la création des fichiers, est ambiguë, et ne précise pas si les données traitées pourront être cédées ou partagées ou quelles personnes pourront y figurer.

Le juge constitutionnel apparaît beaucoup plus contraignant pour les fichiers privés que pour les fichiers publics puisque toutes les carences législatives ne permettent pas de rendre l'intervention de la CNIL suffisante pour assurer la constitutionnalité du dispositif. D'habitude arrimé à des garanties procédurales, le Conseil constitutionnel ne s'en contente pas s'agissant des fichiers privés.

III.5.3. Décision n° 2011-625 DC du 10 mars 2011 – *Loi d'orientation et de programmation pour la performance de la sécurité intérieure*

Le Conseil constitutionnel renforce le contrôle de l'autorité judiciaire sur les données enregistrées dans les fichiers d'antécédents judiciaires.

En matière de fichiers de données, le Conseil constitutionnel a manifesté sa préférence au regard de l'intervention de l'autorité judiciaire. Il considère que le contrôle exercé par un procureur de la République sur les fichiers d'antécédents judiciaires est une garantie de nature

à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'était pas manifestement déséquilibrée.

III.5.4. Décision n° 2012-652 DC du 22 mars 2012 – *Loi relative à la protection de l'identité*

Le Conseil constitutionnel se prononce sur les implications d'un « droit à la protection des données personnelles ». Dans un considérant de principe de portée générale, il a retenu que « la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiées par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif ». Le juge constitutionnel consacre donc un principe de finalité (les fichiers doivent viser un objectif d'intérêt général) et un principe de proportionnalité (les techniques employées doivent être proportionnées à l'objectif à atteindre).

Ces garanties sont toutes destinées à assurer le respect du droit au secret de la vie privée rattaché à l'article 2 de la Déclaration des droits de l'homme et du citoyen. Ainsi, si le droit à la protection des données personnelles existe dans la jurisprudence du Conseil constitutionnel, sa garantie ne vaudra qu'aussi longtemps qu'il existera un risque d'atteinte au droit au respect de la vie privée.

Dans cette décision, le Conseil a reconnu que « la création d'un traitement de données à caractère personnel destiné à préserver l'intégrité des données nécessaires à la délivrance des titres d'identité et de voyage [qui] permet de sécuriser la délivrance de ces titres et d'améliorer l'efficacité de la lutte contre la fraude » est « justifiée par un motif d'intérêt général » (cons.9). Il a toutefois estimé que, compte tenu des quatre caractéristiques du dispositif (ampleur du fichier[32], sensibilité des données, caractéristiques techniques permettant l'identification à partir des données biométriques et finalités de police administrative ou judiciaire autres que celles nécessaires à la délivrance ou au renouvellement des titres d'identité et de voyage et à la vérification de l'identité du possesseur d'un tel titre), l'instauration d'un tel traitement de données à caractère personnel portait une atteinte au respect de la vie privée qui ne pouvait être regardée comme proportionnée au but poursuivi.

Dans le prolongement du commentaire officiel de la décision, il convient de souligner que : « [p]ar cette décision, le Conseil constitutionnel ne s'est pas prononcé pour ou contre la biométrie. Il ne s'est pas davantage prononcé pour ou contre un fichier réunissant des données biométriques »[33]. Il a estimé les garanties offertes insuffisantes.

III.5.5. Décision n° 2016-536 QPC du 19 février 2016 – *Ligue des droits de l'homme* [Perquisitions et saisies administratives dans le cadre de l'état d'urgence]

Le Conseil constitutionnel a choisi l'abrogation immédiate de la disposition de la loi du 3 avril 1955 permettant à l'autorité administrative de collecter les données informatiques consultées lors d'une perquisition administrative.

La loi permettait de copier toutes les données informatiques auxquelles l'autorité administrative avait pu accéder, ce qui était assimilable à une saisie. Or, « ni cette saisie ni l'exploitation des données ainsi collectées ne sont autorisées par un juge, y compris lorsque l'occupant du lieu perquisitionné ou le propriétaire des données s'y oppose et alors même

---

[32] Dans le considérant 10, le Conseil souligne que la quasi-totalité de la population française serait concernée.

[33] Commentaire de la décision par le service de communication du Conseil : https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/decisions/2012652dc/ccc_652dc.pdf.

qu'aucune infraction n'est constatée ». Peuvent être copiées « des données dépourvues de lien avec la personne dont le comportement constitue une menace pour la sécurité et l'ordre public ayant fréquenté le lieu où a été ordonnée la perquisition ».

Ce faisant, le législateur n'a pas prévu de garanties propres « à assurer une conciliation équilibrée entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et le droit au respect de la vie privée ».

III.5.6. Décision n° 2016-591 QPC du 21 octobre 2016 – *Mme Helen S.* [Registre public des trusts]

Dans cette décision, le Conseil rappelle que « la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiées par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif ».

Après avoir admis que l'objectif de valeur constitutionnelle de lutte contre la fraude et l'évasion fiscales autorisait le législateur à instaurer un registre des trusts, le juge constitutionnel a conclu au caractère manifestement disproportionné de l'atteinte à la vie privée, en l'absence de limitation du cercle de personnes ayant accès aux données de ce registre, lequel fournissait des informations sur la manière dont les personnes qui y figuraient entendaient disposer de leur patrimoine.

III.5.7. Décision n° 2017-670 QPC du 27 octobre 2017 – *M. Mikhail P.* [Effacement anticipé des données à caractère personnel inscrites dans un fichier de traitement d'antécédents judiciaires]

Le Conseil est sensible à la disproportion qu'il constate entre l'importance du fichier et la limitation du droit à l'effacement des données. D'une part, les personnes fichées sont très nombreuses et, du moins pour un certain nombre, ne sont coupables d'aucune infraction. C'est vrai des personnes relaxées, acquittées ou qui ont bénéficié d'un non-lieu. Mais c'est aussi vrai des victimes qui figurent également dans le fichier de traitement d'antécédents judiciaires (TAJ). Très large dans le fichage, le TAJ est également très ouvert à la consultation. Forces de police et de gendarmerie, magistrats, mais aussi fonctionnaires chargés d'enquêtes purement administratives peuvent l'utiliser. D'autre part, et c'est là que réside le contraste, le droit d'effacement n'est ouvert qu'à un nombre très restreint de personnes. C'est précisément ce contraste que sanctionne le Conseil constitutionnel.

Cette décision marque un durcissement par rapport à la première décision rendue en 2011 sur les fichiers d'antécédents judiciaires. À l'époque, le Conseil n'avait formulé aucune réserve sur la procédure d'effacement dont le champ était identique. Cette évolution trouve sans doute son origine dans l'influence de la jurisprudence de la Cour européenne des droits de l'homme (CEDH) puisque, dans l'arrêt du 18 avril 2013, *M. K. c. France*, la CEDH a sanctionné pour atteinte à la vie privée le Fichier électronique des empreintes digitales (FAED). Il prévoyait en effet une durée de conservation extrêmement longue, vingt-cinq ans, d'autant plus longue que ce fichage pouvait concerner des personnes condamnées, mais aussi d'autres parfaitement innocentes. De même, dans l'arrêt du 18 septembre 2014, *Brunet c. France*, la Cour européenne précise que la procédure d'effacement du Système de traitement des infractions constatées (STIC) doit permettre à l'autorité compétente d'apprécier la proportionnalité du fichage aux finalités du traitement.

III.5.8. Décision n° 2018-765 DC du 12 juin 2018 – *Loi relative à la protection des données personnelles*

Dans cette récente décision, outre que le Conseil confirme le rattachement de la protection des données personnelles au respect de la vie privée (la décision n° 2004-499 DC précitée) sans lui donner un fondement autonome, il valide le nouveau dispositif de la loi de 1978.

L'adaptation de la loi de 1978 au RGPD a conduit à faire disparaître les formalités préalables à la création des traitements. Désormais, le système de protection repose sur l'appréciation des risques par le responsable du traitement lui-même, la CNIL exerçant un contrôle *a posteriori*. Le Conseil constitutionnel a retenu que « le législateur, qui n'était pas tenu de prévoir un dispositif d'autorisation préalable des traitements de données en cause, n'a pas méconnu le droit au respect de la vie privée. Il n'est pas davantage resté en deçà de sa compétence. Les griefs tirés de la méconnaissance de l'article 2 de la Déclaration de 1789 et de l'article 34 de la Constitution doivent ainsi être écartés ».

III.6. Le droit au déréférencement reconnu par les cours suprêmes

Le Conseil d'État, quelques mois après l'entrée en vigueur de la loi pour une République numérique, a consacré un droit au déréférencement des liens c'est-à-dire « à la suppression de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom du demandeur, des liens vers des pages web, publiées par des tiers et contenant des informations » concernant la personne[34]. Quasiment un après, c'est au tour de la Cour de cassation de rendre un arrêt dans lequel elle rappelle que la juridiction saisie d'une demande de déréférencement est tenue « de porter une appréciation sur son bien-fondé, de procéder, de façon concrète, à la mise en balance des intérêts en présence »[35].

[34] CE, ass. 24 fév. 2017, *Mme Chupin et a.*, *RFDA* 2017, conclusions A. Bretonneau, pp. 535.

[35] Civ. 1ère, 14 fév. 2018, n° 17-10.499, *D.* 2018. p. 348.

IV. La nature du droit au respect de la vie privée

IV.1. Le droit fondamental au respect de la vie privée

Le droit au respect de la vie privée est un droit fondamental. Il s'agit donc d'un droit subjectif, inséparable du sujet de droit. Ce droit est opposable en justice et permet aux individus de limiter le pouvoir d'action des tiers. Les nationaux comme les étrangers sont titulaires de ce droit[36]. Il appartient néanmoins au juge constitutionnel de le concilier avec d'autres droits constitutionnels ou/et intérêts légitimes.

Il est désormais amplement admis que les individus sont à présent largement surveillés. La Cour de justice de l'Union européenne l'a ainsi rappelé en évoquant « les données de connexion » qui donnent des indications précises sur la vie privée des personnes notamment sur les habitudes de vie quotidienne, les lieux de séjours, les déplacements et les milieux sociaux fréquentés (CJUE 8 avril 2014, *Digital Rights Ltd*, aff. C-293/12, § 27). En revanche, la protection des données personnelles ne correspond pas en droit français à un droit fondamental. Ce n'est qu'en tant que prolongement d'un droit fondamental (au respect de la vie privée) qu'elle bénéficie d'une protection constitutionnelle.

Deux observations peuvent être formulées : l'une qui regarde les garanties apportées et l'autre relative aux données personnelles.

Concernant les garanties, il convient de souligner que le principe du fichage a échappé jusqu'à présent au contrôle du juge puisque la loi de 1978 instaurait le principe de la déclaration préalable des fichiers (modifié récemment comme rappelé précédemment par la loi du 20 juin 2018 dans le prolongement du RGPD). Le contrôle juridictionnel porte sur les finalités et les modalités d'accès au traitement. Le contrôle d'éventuelles dérogations à l'interdiction de fichage des données sensibles incombe au juge constitutionnel (si le fichier est créé par le législateur comme par exemple, le Fichier National Automatisé des Empreintes Génétiques) ou au juge administratif (si le fichier est créé par voie réglementaire comme par exemple, le Traitement d'Antécédents Judiciaires).

Concernant les données personnelles, la législation française privilégie une approche personnaliste de ces informations personnelles. Tous les rapports (ceux du Conseil d'État, de la CNIL, de la CNCDH et des parlementaires) se prononcent en faveur du maintien de cette approche face à une logique patrimoniale. La reconnaissance d'un droit de propriété de l'individu sur ses données est régulièrement évoquée de manière à lui donner un pouvoir de négociation face aux GAFAM. Elle est toutefois rejetée même si cela ne conduirait pas à une privatisation irréversible des données, car l'action de l'État serait fragilisée en vue de protéger les individus qui pourraient se prévaloir de la valeur constitutionnelle du droit de propriété (et ainsi ils pourraient abuser de leurs propres données). La monétisation des données personnelles romprait l'approche généraliste et personnaliste du droit français qui considère « la donnée personnelle comme le support indirect d'un droit fondamental et inaliénable reconnu à l'individu dont elle émane et non comme un objet économique ".[37] De toute manière, les données individuelles en elles-mêmes n'ont pas véritablement de valeur. Ce n'est qu'une fois traitées et agrégées entre elles qu'elles acquièrent une valeur monétaire. Les

[36] Voir notamment parmi les décisions du Conseil constitutionnel : n° 2003-4884 DC, du 20 novembre 2003 (cons. 11), n° 2013-347 QPC du 11 octobre 2013 (cons.7).

[37] C. Paul et C. Féral-Schuhl, *Numérique et libertés : un nouvel âge démocratique*, Rapport AN, n° 3119, 2015, commission de réflexion et de propositions ad hoc sur le droit et les libertés à l'âge du numérique, p. 132.

données personnelles ne représentent donc pas une ressource dont les individus sont propriétaires, mais uniquement une extension de leur personnalité, dont ils ont le droit de contrôler l'usage et l'exploitation.

IV.2. Un droit fondamental à concilier

Le respect de la vie privée n'est pas absolu. Il doit être concilié avec d'autres droits ou principes constitutionnels légitimes. Si, en principe, les immixtions dans la vie privée sont illicites, il peut exister des ingérences étatiques légitimes, par exemple pour la protection de la liberté d'expression ou la lutte contre le terrorisme ou la sauvegarde de l'ordre public. Il convient de trouver un juste équilibre entre les différents intérêts légitimes. La première étape à affranchir dans le cadre du contrôle de constitutionnalité est donc que le législateur qui entend porter atteinte au respect de la vie privée, doive le justifier par une exigence constitutionnelle ou un intérêt général (non constitutionnel).

Désormais, notre société est massivement numérisée. Cela est dû à de nombreux facteurs, mais principalement au marché. Si, dans un premier temps, les bases de données ont été réalisées par des organismes publics ou parapublics, de nos jours la collecte de données résulte d'abord de l'activité des entreprises privées. En effet, les réseaux sociaux et les moteurs de recherche stockent une quantité et une variété d'informations jusqu'alors inimaginables. Correctement mis en question, même les données les plus inoffensives, une fois recueillies, peuvent révéler des informations sensibles. De telles ressources ont fini par attirer les gouvernements, qui sont de plus en plus à la recherche d'informations pour anticiper les menaces potentielles, en particulier, en matière de la sécurité publique.

Cela explique sans doute que le Conseil constitutionnel ait rendu en 2012 une décision importante à propos de la loi relative à la protection de l'identité (décision n° 2012-652 DC précitée dans la partie précédente) en posant un considérant de principe : « la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiées par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif ». Le juge constitutionnel consacre donc un principe de finalité (les fichiers doivent viser un objectif d'intérêt général) et un principe de proportionnalité (les techniques employées doivent être proportionnées à l'objectif à atteindre). De manière plus générale et dans un second temps, le Conseil met donc en balance les termes de la pesée identifiés et met en œuvre un contrôle de proportionnalité.

De même, le Conseil a rendu une décision importante à propos de la loi sur le renseignement (décision n° 2015-713 DC précitée dans la partie précédente). Cette loi a fragilisé l'équilibre entre le respect du secret des correspondances, composante du droit au respect de la vie privée, et les objectifs notamment de sécurité nationale et de la prévention du terrorisme en permettant la collecte de données en lien avec la surveillance. Le législateur a procédé de manière classique en affichant dès les premières dispositions la balance entre d'une part, les droits constitutionnels et, d'autre part, les intérêts légitimes néanmoins particulièrement vastes. La loi commence par rappeler que « l'autorité publique ne peut porter atteinte [au respect de la vie privée dans toutes ses composantes] que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité ». Sont ensuite énumérées ces hypothèses justifiant l'atteinte portée aux libertés : « 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ; 2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ; 3° Les intérêts économiques, industriels et scientifiques majeurs de la France ; 4° La prévention du terrorisme ; 5° La prévention : a) Des atteintes à la forme républicaine des institutions ; b) Des

actions tendant au maintien ou à la reconstitution de groupements dissous [...] ; c) Des violences collectives de nature à porter gravement atteinte à la paix publique ; 6° La prévention de la criminalité et de la délinquance organisées ; 7° La prévention de la prolifération des armes de destruction massive ».

Ce texte a étendu aux services de renseignement la possibilité de recourir à des moyens de surveillance réservés jusque-là à la police judiciaire[38], notamment la captation et l'enregistrement de données informatiques. Il autorise également le recours à de nouvelles technologies de surveillances (comme par exemple, la pose de fausses antennes relais à proximité de personnes à surveiller afin de capter leurs conversations téléphoniques et échanges électroniques : données de connexion et contenus de correspondance (IMSI Catchers)). Il permet, enfin, un accès administratif aux données de connexion par le biais des interceptions de sécurité (ou écoutes administratives). L'ensemble du dispositif a été jugé conforme à la Constitution puisque ces mesures intrusives sont placées sous le double contrôle d'une nouvelle autorité administrative (la Commission nationale de contrôle des techniques de renseignement) et du Conseil d'État (en formation restreinte habilitée au secret-défense).

Seule la mise en œuvre de la surveillance des communications électroniques internationales a été censurée car le législateur renvoyait les conditions de mise en œuvre de ces techniques de renseignement (conditions d'exploitation, de conservation et de destruction des renseignements collectés, des conditions de traçabilité et de contrôle par la commission) à un simple décret en Conseil d'État. Le législateur a rapidement réagi en proposant un nouveau texte : la loi relative aux mesures de surveillance des communications électroniques internationales du 30 novembre 2015. Le Conseil constitutionnel a jugé dans sa décision n° 2015-722 DC (précitée dans la section précédente) que l'ensemble des dispositions examinées « ne portent pas d'atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances » (cons. 15).

En France, la réforme de l'état d'urgence a suscité trois questions prioritaires de constitutionnalité devant le Conseil constitutionnel. Néanmoins, seule la question prioritaire de constitutionnalité n° 2016-536 (précitée dans la partie précédente) a abrogé le nouvel article 11 de la loi de 1955 sur l'état d'urgence car elle permettait aux policiers de recueillir toutes les données stockées dans les appareils numériques recueillis au cours d'une perquisition à domicile sans mandat de saisie délivré par un juge. De plus, l'article 11 autorisait à procéder au téléchargement des données, quelle que soit leur corrélation avec l'infraction, sans définir de critères comme la durée de leur conservation ou toute norme de sécurité.

De même, la décision n° 2016-590 QPC (précitée dans la section précédente) a été saluée par la doctrine puisque le Conseil constitutionnel a fait disparaître du droit français une disposition vieille de 25 ans et redéployée dans ses effets par la loi relative au renseignement qui permettait aux services de renseignement la surveillance des communications par téléphonie mobile sans autorisation du Premier ministre accordée après avis de la CNCTR.

[38] Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par voie des communications électroniques et la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

V. Conclusions

La révolution numérique induit un déplacement de perspective par l'ampleur incommensurable et la vitesse de propagation croissante des nouveautés technologiques qui défient la compréhension individuelle et l'appréhension collective. Pour les libertés et en tout premier lieu le respect de la vie privée, ce déploiement suppose de s'interroger sur les garanties offertes : le bilan est nuancé, ce qui appelle à renforcer le système de garanties.

V.1. Un bilan à nuancer

Le droit français est-il un rempart suffisamment solide face aux défis digitaux ? Il convient tout d'abord de souligner la dimension transnationale de ces défis. Dès lors, la seule perspective nationale est sans aucun doute insuffisante en raison de la fluidité des objets numériques et du poids des GAFAM[39]. Parce que la question est transnationale et aussi parce qu'elle est évolutive (*i.e.* une question technique par nature changeante), les actuelles et récurrentes discussions autour d'une charte constitutionnelle du numérique semblent sans issue : la rédaction d'une telle charte est prématurée. On observera d'ailleurs qu'une telle option a été écartée dans le cadre de la révision constitutionnelle en discussion devant le parlement en juillet 2018. En revanche, une reconnaissance constitutionnelle explicite et séparée des droits au respect de la vie privée et de la protection des données personnelles pourrait à la fois clarifier le fondement constitutionnel de ces droits dans le prolongement de la jurisprudence développée et donner ainsi une assise plus ferme à ces droits lors de la balance avec des intérêts légitimes tels que la sécurité publique.

Cette solution est assez largement partagée par les acteurs du secteur et la doctrine. Par exemple, l'actuelle présidente de la CNIL, Isabelle Falque-Pierrotin, s'est prononcée à plusieurs reprises en faveur de cette solution. Ainsi, avance-t-elle que les données personnelles sont devenues l'une des composantes à part entière de l'identité et de la personnalité des individus, qui méritent d'être protégées comme telles même lorsqu'elles ne touchent pas au cœur de l'intimité de leur vie privée[40]. L'idée très largement défendue est de s'aligner sur le standard de protection le plus élevé en Europe et donc de reconnaître le droit à l'autodétermination informationnelle des individus, à l'instar de la Cour constitutionnelle allemande avec son arrêt fondateur de 1983. À l'occasion de l'examen de la loi sur le recensement, la Cour allemande a déduit ce droit des articles 1er (dignité humaine) et 2 (droit au libre développement de sa personnalité). Elle a ainsi formulé ce droit nouveau : "la Constitution garantit en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel"[41].

En particulier, la reconnaissance constitutionnelle du droit à la protection des données personnelles permettrait d'élever les conditions d'exploitation des données personnelles en soumettant leur traitement à l'exigence de loyauté et à l'existence de fins déterminées ainsi que d'un fondement légitime ou du consentement de l'intéressé. Par ricochet, elle devrait également protéger à un haut niveau le droit pour la personne concernée à accéder aux données collectées qui la concernent et le droit d'en obtenir la rectification au sens large. Elle devrait enfin garantir le contrôle du respect de ces règles par une autorité indépendante et

[39] La condamnation le 17 mai 2017 par la CNIL de Facebook pour atteinte à la vie privée, en raison de la « combinaison potentiellement illimitée de toutes les données des utilisateurs », manifeste une volonté nouvelle de s'attaquer aux dérives des GAFAM, mais dont la portée reste limitée.

[40] I. Falque-Pierrotin, « La Constitution et l'Internet », *NCCC*, 2012, n° 36, p. 36.

[41] Cité dans le rapport du Conseil d'État précité, p. 267.

impartiale. Une telle consécration permettrait, pour ce qui concerne son volet numérique, de mieux protéger notamment le droit au secret des correspondances numériques et le droit à l'inviolabilité du domicile numérique face à certaines technologies intrusives. Avec le droit à l'autodétermination informationnelle, il s'agit d'aller plus loin en donnant à l'individu "la possibilité de reprendre la maîtrise sur [la] dispersion de ses données et d'affermir le lien entre l'individu et son double numérique. Pour cela, la seule version défensive de la protection des données personnelles ne suffit plus ; il faut ajouter un versant plus positif […]".[42] Il s'agirait de renforcer les moyens dont dispose l'individu pour qu'il maîtrise la gestion de ses données et donc la double face de ce droit à l'ère digitale : exposer publiquement ses données personnelles et protéger sa vie privée. L'article 1er de la loi Informatique et Liberté a été ainsi complété par la loi pour une République numérique (2016) : « toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant ».

Néanmoins, une reconnaissance constitutionnelle expresse n'est pas forcément nécessaire puisque la protection des droits fondamentaux est évolutive : les tâtonnements de la jurisprudence constitutionnelle à propos du fondement du droit au respect à la vie privée en témoignent et le Conseil constitutionnel pourrait donc la faire évoluer en recomposant la liste des droits reconnus, voire en constitutionalisant la grande loi de 1978[43]. L'intensité de la protection de la vie privée est discutée en doctrine, les décisions constitutionnelles de censure n'étant pas légion. Néanmoins, tous s'accordent à reconnaître que ce droit reconnu tardivement en droit français a désormais une place importante dans la jurisprudence constitutionnelle.

V.2. Un système de garanties à renforcer

À côté des garanties juridiques, c'est aussi une autre perspective qui semble se dessiner. En effet, les risques liés à l'usage de l'outil numérique ont conduit à développer une protection de type technique : en prenant en compte la protection des données personnelles dès la phase de conception des systèmes informatiques (*privacy by design*), le niveau de protection est élevé dans la phase conceptuelle de manière à réduire le nombre de données nécessaires au traitement projeté et le risque de mésusage des données par des tiers. Cette régulation ne repose plus sur l'intervention *a posteriori* d'une autorité publique. Le RGDP a adopté cette approche de manière à concrétiser la maîtrise des données personnelles par les internautes eux-mêmes. Un exemple est la pseudonymisation. C'est une procédure de gestion et de désidentification des données par laquelle les informations personnellement identifiables dans un enregistrement de données sont remplacées par des identifiants artificiels (pseudonymes). Même s'il convient au traitement des données, l'enregistrement lui-même est moins identifiable et nécessite des informations supplémentaires conservées séparément pour être parfaitement compréhensible. Cette procédure est fortement encouragée par le nouveau règlement européen 2016/679, qui offre ainsi une vision intégrée de la protection de la vie privée (juridique et technique). Un autre outil est la minimisation des données, selon laquelle seules les données strictement liées au but pour lequel elles sont données peuvent être collectées. La minimisation est liée à la fois à leur utilisation ultérieure et à leur temps de

[42] I. Falque-Pierrotin, *op.cit.*, p. 37. Voir aussi le rapport du Conseil d'État, précité, pp. 264.

[43] Voir sur la liste ouverte des droits constitutionnels, M.-C. Ponthoreau, *La reconnaissance des droits non écrits par les cours constitutionnelles italienne et française. Essai sur le pouvoir créateur du juge constitutionnel*, Paris, Economica, 1993.

rétention, qui connaissent la même limite de l'objectif pour lequel elles ont été données par la personne concernée.

Cette promotion des technologies protectrices de la vie privée et des données personnelles ouvre un nouveau champ pour la régulation par la CNIL. Elle est désormais compétente selon l'article 11 de la loi de 1978 : « Elle promeut, dans le cadre de ses missions, l'utilisation des technologies de la vie privée, notamment les technologies de chiffrement des données » (point 4. F.). Dès la loi pour la République numérique, cette nouvelle compétence a été introduite de manière à parer à l'ouverture maximale des données publiques. Le Conseil d'État avait souligné dans son rapport précité qu'il convenait de « prévenir les risques pour la vie privée », en définissant de « bonnes pratiques d'anonymisation », en vue de « limiter les risques de ré-identification »[44]. De ces nouvelles directions prises en vue de protéger les individus, il ressort que ces derniers ne sont pas forcément les mieux armés pour se défendre contre d'éventuels abus car ils sont prêts à céder leurs données personnelles pour des avantages immédiats. Sans conscience de la gravité des risques ultérieurs d'atteinte à la vie privée, il faut donc envisager aussi de les protéger contre eux-mêmes. Parmi les nouveaux droits souvent évoqués pour figurer dans une charte du numérique, le droit à l'éducation et à l'information du numérique devrait y figurer en bonne place précisément pour renforcer la conscience des menaces qui pèsent sur la vie privée à l'ère digitale.

L'équilibre difficile à trouver entre liberté et sécurité, d'une part, et la tendance sans cesse grandissante de la publicisation des données, d'autre part, appellent à la plus grande vigilance puisque la marge d'autonomie individuelle se réduit. La convergence des solutions nationale et européenne joue sans doute de manière bénéfique en faveur d'un renforcement des systèmes de garanties. Cela sera-t-il suffisant pour se protéger des " bouleversements de tous ordres induits par une révolution numérique qui atteint tous les éléments constitutifs de l'ordre social " dont " l'inflexion de la conception traditionnelle de la vie privée n'est qu'un des aspects "[45] ? La révolution numérique induit un tel déplacement de perspective que seuls des doutes peuvent être émis.

[44] Rapport, *op.cit*., p. 309. Dans le même sens, G. Gorce, F. Pillet, *L'Open data et la protection de la vie privée,* Rapport d'information, Sénat, n° 469, 2014.

[45] J. Chevalier, « La vie privée à l'épreuve de la société numérique », *in Mélanges en l'honneur d'Elisabeth Zoller*, 2018, à paraître.

Liste des lois françaises en relation avec le droit au respect de la vie privée

Loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

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

Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique

Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles

Liste d'arrêts

Arrêt de la Cour de justice de l'Union européenne

C.J.U.E., 8 avril 2014, *Digital Rights Ltd*, C-293/12

C.J.U.E., 13 Mai 2014, *Google Spain*, C-131/12

Arrêts de la Cour européenne des droits de l'homme

Cour EDH, 16 décembre 1992, *Niemetz c. Allemagne*, n° 13710/88

Cour EDH, Grande chambre*, S. et Marper c. Royaume-Uni*, 4 décembre 2008, n° 30562/04 et 30566/04.

Cour EDH, 18 septembre 2014, *Brunet c. France*

Cour EDH, 18 avril 2013 *M. K. c. France*

Arrêts de cours étrangères

Cour constitutionnelle allemande, 15 décembre 1983, *Loi sur le recensement*

Cour suprême des États-Unis, 1965, *Griswold v. Connecticut*, 381 US 479

Décisions du Conseil constitutionnel français

Décision n° 92-316 DC du 20 janvier 1993 – *Loi relative à la prévention de la corruption et à la transparence de la vie économique et des procédures publique*

Décision n° 93-325 DC du 13 août 1993 – *Loi relative à la maîtrise de l'immigration et aux conditions d'entrée, d'accueil et de séjour des étrangers en France*

Décision n° 94-352 DC du 18 janvier 1995 – *Loi d'orientation et de programmation relative à la sécurité*

Décision n° 99-416 DC du 23 juillet 1999 – *Loi portant création d'une couverture maladie universelle*

Décision 2004-492 DC du 2 mars 2004 – *Loi portant adaptation de la justice aux évolutions de la criminalité*

Décision n° 2004-499 DC du 29 juillet 2004 – *Loi 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*

Décision n° 2004-504 DC du 12 août 2004 – *Loi relative à l'assurance maladie*

Décision n° 2009-580 DC du 10 juin 2009 – *Loi favorisant la diffusion et la protection de la création sur internet*

Décision n° 2010-25 QPC du 16 septembre 2010 – *M. Jean-Victor C. [Fichier empreintes génétiques]*

Décision n° 2011-625 DC du 10 mars 2011 – *Loi d'orientation et de programmation pour la performance de la sécurité intérieure*

Décision n° 2012-652 DC du 22 mars 2012 – *Loi relative à la protection de l'identité*

Décision n° 2015-713 DC du 23 juillet 2015 – *Loi sur le renseignement*

Décision n° 2015-722 DC du 26 novembre 2015 – *Loi relative aux mesures de surveillance des communications électroniques internationales*

Décision n° 2016-536 QPC du 19 février 2016 – *Ligue des droits de l'homme* [Perquisitions et saisies administratives dans le cadre de l'état d'urgence]

Décision n° 2016-590 QPC du 21 octobre 2016 – *La Quadrature du Net et autres* [Surveillance et contrôle des transmissions empruntant la voie hertzienne]

Décision n° 2016-591 QPC du 21 octobre 2016 – *Mme Helen S.* [Registre public des trusts]

Décision n° 2017-670 QPC du 27 octobre 2017 – *M. Mikhail P.* [Effacement anticipé des données à caractère personnel inscrites dans un fichier de traitement d'antécédents judiciaires]

Décision 2018-696 QPC du 30 mars 2018 – *M. Malek B.* [Pénalisation du refus de remettre aux autorités judiciaires la convention secrète de déchiffrement d'un moyen de cryptologie]

Décision n° 2018-765 DC du 12 juin 2018 – *Loi relative à la protection des données personnelles*

Arrêts de Cours suprêmes françaises

CE, ass. 24 fév. 2017, *Mme Chupin et a*.

Cass. civ. 1ère, 14 fév. 2018, n° 17-10.499

Bibliographie

Ouvrages :

BOBBIO N., *L'età dei diritti*, Turin, Einaudi,1992

BOUCIER D., DE FILIPPI P., *Open data et Big data. Nouveaux défis pour la vie privée*, Paris, Mare et Martin, 2016

CARBONNIER J., *Droit civil*, vol.1, Paris, P.U.F., 2004

GARAPON A., LASSEGUE J., *Justice digitale*, Paris, PUF, 2018

HENNETTE-VAUCHEZ S. et ROMAN D., *Droits l'homme et libertés fondamentales*, Paris, Dalloz, 3e éd., 2017

KAYSER P., *La protection de la vie privée par le droit : protection du secret de la vie privée*, Paris-Marseille, PUAM, 3e éd., 1995

PONTHOREAU M.-C., *La reconnaissance des droits non écrits par les cours constitutionnelles italienne et française. Essai sur le pouvoir créateur du juge constitutionnel*, Paris, Economica, 1993

TÜRK A., *La vie privée en péril*, Paris, Odile Jacob, 2011

WACHSMANN P., *Libertés publiques*, Paris, Dalloz, 8e éd., 2017

Articles :

ANTIPPAS J. et BEIGNIER B., « La protection de la vie privée » in R. CABRILLAC (dir.), *Libertés et droits fondamentaux*, Paris, Dalloz, 24e éd., 2018, pp. 221-263.

BENSAMOUN A., « Les droits fondamentaux et Internet », in R. CABRILLAC (dir.), *Libertés et droits fondamentaux*, Paris, Dalloz, 24e éd., 2018, pp.331-354

BENSAMOUN A., LOISEAU G., « La gestion des risques de l'intelligence artificielle : de l'éthique à la responsabilité », *JCP G*, 2017, n° 46, pp. 2063-2072

BRETONNEAU A. « Le droit au « déréférencement » et la directive sur la protection des données personnelles », *RFDA*, 2017, pp. 535-549

BRETONNEAU A., « Le droit au « déréférencement » : champ territorial », *RFDA*, 2017, pp. 972-981

CHEVALIER J., « Le droit français et la question des données publiques », in D. BOUCIER et P. DE FILIPPI, *Open data et Big data. Nouveaux défis pour la vie privée,* Mare et Martin, 2016, pp. 35-55

CHEVALIER J., « La vie privée à l'épreuve de la société numérique », *in Mélanges en l'honneur d'Elisabeth Zoller*, 2018, à paraître.

CLUZEL-METAYER L., « La loi pour une République numérique : l'écosystème de la donnée saisi par le droit », *AJDA*, 20 fév. 2017, pp.340-345

CYTERMANN L., « La loi Informatique et Libertés est-elle dépassée ? », *RFDA,* 2015, pp. 99-111

DE FILIPPI P., « Gouvernance algorithmique : vie privée et autonomie individuelle à l'ère du *Big data* », in D. BOUCIER et P. DE FILIPPI, *Open data et Big data. Nouveaux défis pour la vie privée,* Mare et Martin, 2016, pp. 99-128.

DEROULEZ J., « Protection et sécurité des données personnelles : premiers avertissements de la CNIL », *JCP G*, 2017, n° 42, pp. 1982-1895

DUCLERCQ J.-B., « Le droit public à l'ère des algorithmes », *RDP*, 2017, n° 5, pp. 1401-1433

FALQUE-PIERROTIN I., « La Constitution et l'Internet », *NCCC*, 2012, n° 36, pp. 31-44

GEFFRAY E., « Droits fondamentaux et innovation : quelle régulation à l'ère du numérique », *NCCC*, 2016, n° 52, pp. 5-16

HALPERIN J.-L., « L'essor de la "*privacy*" et l'usage des concepts juridiques », *Droit et Société*, 2005, n° 61, pp. 765-782.

HALPERIN J.-L., « Protection de la vie privée et privacy : deux traditions juridiques différentes ? », *NCCC*, 2015, n° 48, pp. 59-68

LANNA M., « Les objets connectés : entre remise en question de la notion de vie privée et évolution du droit des traitements des données personnelles », *RDP*, 2017, n° 5, pp. 1435-1447

MARTIN V., « La République numérique en débat au Parlement : le projet de commissariat à la souveraineté numérique », *NCCC*, 2017, n° 57, pp. 107-109

MASTOR W., « La loi sur le renseignement du 24 juillet 2015 », AJDA, 2015, pp. 2018-2024

MAZEAUD V., « La constitutionnalisation du droit au respect de la vie privée », *NCCC*, 2017, n° 48, pp.7-20

OCHOA N., « Pour en finir avec l'idée d'un droit de propriété sur ses données : ce que cache véritablement le principe de libre disposition », *RFDA*, 2015, pp. 1157-1173

OBERDORFF H., « L'espace numérique et la protection des données personnelles au regard droits fondamentaux », *RDP*, 2016, n° 1, pp. 41-54

PEYROU S., « La protection des données à caractères personnel au sein de l'UE : des enjeux économiques et sécuritaires encadrés par le législateur sous le contrôle du juge », *RDP*, 2016, n° 1, pp. 55-69

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, pp. 125-138

QUÉMÉNER M., « Les données personnelles à l'ère du numérique. Quelle protection sur le plan pénal », *RDP*, 2016, n° 1, pp. 71-86

RICHARD J., « Le numérique et les données personnelles : quels risques, quelles potentialités ? », *RDP*, 2016, n° 1, pp. 87-100

SCOFFONI G., « Le renouveau du droit au respect de la vie privée aux États-Unis : la Cour suprême face aux défis des nouvelles technologies », *in Mélanges en l'honneur d'Elisabeth Zoller*, 2018, à paraître.

TURK P., BONNET J., « Le numérique : un défi pour le droit constitutionnel », *NCCC*, 2017, n° 57, pp. 13-24

SAINT-PAU J.-C., « Droit au respect de la vie privée. Définition conceptuelle du droit subjectif », *Juris-Classeur Communication*, mise à jour 25 février 2018, Fascicule 34

WARREN S.D., BRANDEIS L.D., « The Right to Privacy », 4 *Harvard Law Review*, 1890, pp. 193-220

ZOLLER E., « Le droit au respect de la vie privée aux États-Unis » in F. SUDRE (dir.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruxelles, Bruylant, Coll. Droit et Justice n° 63, 2005, pp. 35-67

Rapports :

Avis de la CNCDH du 22 mai 2018 sur la "Protection de la vie privée à l'ère numérique" *JORF* du 3 juin 2018 (texte n° 6)

CADIET L., *L'open data des décisions de justice*, Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice, Rapport remis à la garde des Sceaux le 9 janvier 2017

GORCE G., PILLET F., *L'Open data et la protection de la vie privée,* Rapport d'information, Sénat, n° 469, 2014

PAUL C., FERAL-SCHUHL C., *Numérique et libertés : un nouvel âge démocratique*, Commission de réflexion et de propositions ad hoc sur le droit et les libertés à l'âge du numérique, Rapport AN, n° 3119, 2015

Rapport du Conseil d'État, *Le numérique et les droits fondamentaux,* La Documentation française, n° 64, 2014

Principaux sites internet consultés

Site de l'Assemblée nationale : http://www.assemblee-nationale.fr

Site de la Commission nationale Informatique et Libertés : https://www.cnil.fr

Site de la Commission nationale consultative des droits de l'homme : http://www.cncdh.fr/fr/publications

Site du Conseil constitutionnel : http://www.conseil-constitutionnel.fr

Site du Conseil d'État : http://www.conseil-etat.fr

Site du journal officiel : http://www.journal-officiel.gouv.fr

Site du ministère de la justice : http://www.justice.gouv.fr/

Site du Sénat : http://www.senat.fr

QA-04-18-839-FR-N

La présente étude fait partie d'un projet plus général qui vise à jeter les bases d'une comparaison des régimes juridiques applicables au droit au respect de la vie privée dans les différents ordres juridiques, ainsi que des solutions prévues par ces ordres juridiques pour répondre aux enjeux que l'« ère digitale » pose à ce droit.

La publication expose, relativement à la France et en rapport avec le thème de l'étude, la législation en vigueur, la jurisprudence la plus pertinente et la nature du droit au respect de la vie privée, et s'achèvent par quelques conclusions sur les enjeux précités.

Reconnu tardivement en droit français, le droit au respect de la vie privée a été consacré par le législateur en 1970. Au contenu insaisissable, ce droit a été adapté aux évolutions technologiques de manière à poser des limites aux intrusions dans la sphère privée : tout d'abord face aux avancées de l'informatique avec la grande loi de 1978, puis à celles du numérique en adaptant cette même loi. Bien que la Constitution de 1958 reste silencieuse, le Conseil constitutionnel a consacré comme fondamental le droit au respect de la vie privée et pose des limites aux intrusions dans la sphère privée.

Publication de l'Unité Bibliothèque de droit comparé
EPRS | Service de recherche du Parlement européen

Papier ISBN 978-92-846-3917-5 | doi:10.2861/231598 | QA-04-18-839-FR-C
PDF ISBN 978-92-846-3915-1 | doi:10.2861/779730 | QA-04-18-839-FR-N